CITI STANDARDS FOR SUPPLIERS

OWNER:
GLOBAL HEAD OF ENTERPRISE SUPPLY CHAIN

ISSUE DATE:
JANUARY 2015

REVISED:
JANUARY 11, 2019

VERSION:
3.0

TABLE OF CONTENTS

1 GENERAL OVERVIEW 1
2 CITI GUIDING PRINCIPLES, ANTI-BRIBERY AND ETHICAL CONDUCT 4
3 ACCESSIBILITY AND DIVERSITY 19
4 ENVIRONMENTAL SUSTAINABILITY 20
5 SUPPLIER RELATIONSHIP AND CONTRACT COMPLIANCE 23
6 EXPENSES 26
7 GIFTS AND ENTERTAINMENT 33
8 RECORDS MANAGEMENT 34
9 SECURE WORKPLACE GUIDELINES 35
10 INFORMATION SECURITY (IS) 36
11 CONTINUITY OF BUSINESS 56
12 GLOBAL COMPLAINTS / CONCERNS MANAGEMENT STANDARDS 60
13 GLOBAL BACKGROUND SCREENING STANDARDS 63
APPENDIX A - DEFINITIONS 68

1 GENERAL OVERVIEW

1.1 PURPOSE

The purpose of the Citi Standards for Suppliers ("Standards") is to facilitate Suppliers' compliance with contractual requirements and ensure that Suppliers comply with Citi policy obligations in the course of doing business with Citi.

a. Failure to comply with the Standards set forth in this document, other Citi policies, Citi's Code of Conduct and / or the policies and procedures applicable to the Citi business and legal entity for which a Supplier is providing products and / or services may result in material default (and consequently, lead to termination for cause) of a Supplier's engagement with Citi, including any and all agreements related thereto, and / or other contractual consequences. Furthermore, violations of the Standards may also be violations of applicable law and may result in civil damages owed to Citi (or third parties) or criminal penalties for the Supplier.

b. These Standards provide a key general overview of Citi's policy requirements with which Suppliers must comply. It is not meant to be an all-inclusive list of standards and requirements. Each Citi business and legal entity may also indicate in the transactional document (work order or license) additional, policies and standards with which Suppliers must comply. Banks, broker-dealers and other licensed Citi entities in particular are subject to specific requirements and limitations based on the nature of their regulated activity(ies) being conducted. These requirements and limitations are reflected in business-specific policies, including any policies applicable to such entities' Suppliers. In the event such entity-specific policies differ from these Standards with respect to the same topic, the more restrictive policy will prevail in order of interpretation. It is the Supplier's responsibility to become familiar with and adhere to any supplemental Citi policies and procedures agreed by the Supplier and by the Citi business and legal entity for products and services to that business or entity.

c. Suppliers must take a proactive role and consult with their primary Citi business contact (or his or her designee) regarding any questions they may have in respect to Citi policies to help ensure compliance with current Citi policies, or any changes as notified.

d. If a Supplier has any reason to believe that any Citi employee, or anyone working on Citi's behalf, may have engaged in actual or potential misconduct, including the failure to comply with the Standards set forth in this document, other Citi policies, Citi's Code of Conduct and / or the policies and procedures applicable to the Citi business and legal entity for which a Supplier is providing products and / or services, the Supplier must promptly report such concerns to their primary Citi business contact and / or any of the contacts listed in Citi's Code of Conduct.

e. These Standards are not intended to invalidate or interfere with any practices or procedures that a Supplier may have which are supplemental to the requirements outlined in these Standards, provided such practices or procedures do not conflict with the requirements of these Standards. If the

Supplier has a related policy or procedure that is more stringent or rigorous than the requirements of Citi's policies, Supplier may comply with the more stringent terms of its own policy, provided that at all times, it still maintains full compliance with these Standards.

f. In some cases, a Supplier's policies address a requirement of these Standards in an alternative way, but one which Supplier's management warrants is substantively and / or functionally equivalent to the requirements of these Standards. Suppliers may not use compliance with its own standards or policies to substitute with the obligation to comply with any provisions of these Standards without Citi's written consent. In requesting to rely, and when relying, on compliance with its own standards or policies in lieu of compliance with any provisions of these Standards, Supplier agrees to work with Citi's management to discuss any questions or concerns that Citi may have with regard to Supplier's alternative approach and shall work in good faith with Citi to ensure that industry and regulatory requirements applicable to Citi are met. In the event that, in Citi's determination, the Supplier policies or practices do not, at a minimum, meet these Standards or any other relevant Citi policy(ies), then Supplier shall take all necessary measures to ensure compliance with these Standards and other relevant Citi policy(ies).

g. If local laws or regulations establish a higher standard than provided here, Suppliers must comply with those laws and regulations. If local laws or regulations appear to conflict with these Standards, the affected Supplier must inform its primary Citi business contact (or his or her designee) and work in good faith with Citi to reach a mutually agreeable resolution that ensures compliance with the relevant law(s) or regulation(s) and, to the extent possible, these Standards.

h. The applicability of these Standards shall be in addition to and not in lieu of, any and all other obligations, covenants or warranties that Suppliers may have to Citi under any Contract or otherwise at law or in equity and any rights and remedies of Citi set forth herein shall be in addition to and not in lieu of any other contractual, legal or equitable rights or remedies that Citi may have with respect to any Supplier(s) or any other party(ies).

i. These Standards may be modified, amended or revised by Citi at any time at Citi's sole discretion and notified to the Suppliers. Where the changes are material, Suppliers shall notify Citi if they disagree or are unable to comply, noting always that changes may be due to a change of applicable law, regulatory activity, or may be contractually required and must be accepted to engage in the purchase of new deliverables or services or the continuation of existing services.

j. These Standards (and any updates) are posted on Citigroup.com:

   http://www.citigroup.com/citi/suppliers/supplierstandards.htm

   The Citi Code of Conduct and any updates are posted on Citigroup.com: http://www.citigroup.com/citi/investor/corporate_governance.html (under Citi Policies).

1.2 Parties Subject to the Standards

These Standards apply to all Suppliers, defined as any third party, together with its employees, agents or representatives, that provide products or services to Citigroup Inc. or any of its Affiliates, including its subsidiaries (collectively or individually, such entities being referred to herein as “Citi” or the “Company”), or any of Citi’s Clients, but only in connection with their activities as a Supplier. Where these Standards contain references to service or products being provided to Citi, or similar references, those should be interpreted to include the provision of goods and services to Citi’s Clients whether on behalf of Citi or with Citi’s facilitation.

In addition, the Suppliers guarantee that they and any sub-contractors they engage: (a) in connection with the provision of Suppliers’ services to Citi or its Clients or (b) with whom Supplier shares any Citi Confidential Information (or potential access to such Citi Confidential Information), comply (and will procure its sub-contractors’ compliance) with all terms of these Standards and any other Citi policies and procedures that may be applicable. Any specific mention of, or terms with respect to, sub-contractors in these Standards (or any specific mention of, or terms with respect to Suppliers’ obligations regarding such sub-contractors) is for emphasis only and does not limit Suppliers’ obligations with respect to its sub-contractors, which include ensuring sub-contractor compliance with any and all other obligations of Suppliers under these Standards.

2 CITI GUIDING PRINCIPLES, ANTI-BRIBERY AND ETHICAL CONDUCT

Citi has adopted certain frameworks (such as the Committee of Sponsoring Organizations of the Treadway Commission (COSO) 2013) and guidelines (i.e., Citi Statement of Supplier Principles, Citi Standards for Suppliers) that support the operational risk management framework, requiring Third Parties to promote social responsibility, ethical business practices, human rights in the workplace and environmental sustainability. In the U.S. and other countries, where appropriate, Citi encourages the utilization of diverse Third Parties and is committed to assisting such Third Parties in their growth and development on a long-term basis.

All Citi Suppliers are required to avoid any situations in which personal interests may conflict or may appear to conflict, with the interests of Citi or its Clients. All Citi Suppliers must always demonstrate commitment to the highest standards of ethics and professional behavior, as well as adhere to all applicable laws and regulations. Additional information about Citi's Statement of Supplier Principles can be found in Citi's Statement of Supplier Principles.

2.1 Mission and Value Proposition

Citi's mission is to serve as a trusted partner to its Clients by responsibly providing financial services that enable growth and economic progress, while earning and maintaining the public's trust by constantly adhering to the highest ethical standards. Under Citi's Mission and Value Proposition, Citi asks its employees to ensure that their decisions pass three tests:

a. they are in our Clients' interests,
b. they create economic value, and
c. they are always systemically responsible.

Citi expects each of its Supplier's decisions with respect to the services and products each provides to Citi or its Clients to pass these three tests also.

2.2 Fair Treatment

Citi is committed to dealing fairly with its Clients, Suppliers, competitors and employees. Citi is also committed to providing fair access to credit and to make credit decisions based on objective criteria. In addition, Citi follows the laws and regulations that specifically prohibit discrimination against prospective or actual Clients on the basis of race, sex, religion or other non-risk factors. No Supplier acting on behalf of Citi or its Clients may take (or attempt to take) unfair advantage of anyone through manipulation, concealment, through use or misuse of Confidential Information, misrepresentation of material facts or other unfair dealings or practices.

2.3 Compliance and Conduct Risk

Guided by Citi's Mission and Value Proposition and the principle of Responsible Finance – conduct that is transparent, prudent, and dependable – Citi seeks to drive and embed a firm-wide risk culture to minimize, mitigate, and manage compliance risk and conduct risk. Compliance risk is the risk arising from violations of, or non-conformance with, local, national, or cross-border laws, rules, or regulations, Citi's

internal policies and procedures, or relevant standards of conduct. For Citi, conduct risk (which is articulated in Citi's Conduct Risk Policy) is the risk that Citi's employees or agents, including Suppliers, may – intentionally or through negligence – harm customers, Clients, or the integrity of the markets, and thereby the integrity of the firm. Suppliers must exercise caution and sound judgment in all aspects of their work to minimize, mitigate, and manage compliance and conduct risk.

2.4 Escalation of Business Concerns

In every action and all aspects of their work, Suppliers must exercise appropriate judgment and common sense in order to assess the potential impact of transactions, activities, or other practices in which they engage on behalf of Citi. Suppliers must immediately escalate to their respective primary Citi business contact and Citi Senior Country Operating Officer any concerns regarding potential franchise, reputational, conduct, or systemic risk issues, each of whom may escalate further to the appropriate business or regional Business Practices Committee.

2.5 Free and Fair Markets

Citi will not tolerate any attempt by a Supplier to manipulate or tamper with the markets or the prices of securities, options, futures or other financial instruments.

2.6 Protecting Citi Assets

Suppliers must safeguard the tangible and intangible assets of Citi and its Clients. Citi and Client assets may be used only for approved purposes and in approved manners (e.g., in accordance with applicable licenses, terms and conditions) and then only with respect to the business purposes of Citi and Citi's Affiliates. Assets include cash, securities, physical property, services, business plans, Citi Information, supplier information, distributor information, intellectual property (computer programs, models and other items) and all other personal, proprietary and Confidential Information.

Misappropriation or unauthorized disclosure of Citi assets is a breach of your duty to Citi and may constitute an act of fraud against Citi. Similarly, carelessness, waste or unauthorized use in regard to Citi assets is also a breach of your duty to Citi. See Secure Workplace Guidelines in Section 9 of these Standards.

2.7 Anti-Bribery

Citi has policies, procedures and internal controls for complying with anti-bribery and corruption laws and prohibits any improper payment, promise of payment, offer of employment, or the improper provision of anything of value, directly or indirectly, to (i) any person employed by, or serving under, a public body, regardless of whether in a legislative, administrative, judicial, executive or military position (whether appointed or elected) or exercise a public function for any such jurisdiction, any public agency or any public enterprise (including any officer, official, employee or agent of any government, any government-owned or government-controlled entity or any public international organization or any person acting in an official capacity for or on behalf of any government entity) in any country or territory, (ii) any political party, party official or candidate for public office, (*((i) and (ii) collectively referred to

as “Government Officials”)) or (iii) any other person for the purpose of obtaining or retaining business or influencing official action.

Citi’s Anti-Bribery Policy requires compliance with applicable law[1] and strictly prohibits bribery in any form. All of Citi’s Suppliers are expected to conduct their activities related to Citi’s business and operations in accordance with high standards of business conduct, which includes compliance with all applicable laws prohibiting bribery, corruption, fraud and false statements and avoidance of even the appearance of wrongdoing or impropriety. Citi’s Anti-bribery Policy prohibits the provision of facilitation payments of any kind. Suppliers shall ensure that appropriate policies and procedures are in place to comply with all applicable laws.

Under no circumstances may a Supplier, or any of its Personnel make or offer to make, promise or grant, accept or request, anything of value (including any advantage, financial or otherwise, such as (without limitation) gifts, entertainment, charitable or political contributions or employment), -to or from-, a Government Official or any other person, on behalf of Citi, whether directly or indirectly through a third party (e.g., family member, an intermediary or agent or an organization) for the purpose of securing improper advantage, influencing the recipient to take, or refrain from taking, any official action or obtaining or retaining business for Citi. Supplier shall not provide facilitation or “grease” payments of any kind.[1]

For an overview of Citi’s Anti-Bribery Program, please visit http://www.citigroup.com/citi/investor/corporate_governance.html (under Citi Policies, select Anti-Bribery Program).

2.8 Anti-Money Laundering (“AML”) Compliance

Money laundering is the process of converting illegal proceeds so that funds are made to appear legitimate and thereby enter the stream of commerce. Terrorist financing includes the financing of terrorist acts and terrorist organizations and may involve proceeds from both illegitimate and legitimate sources. Money laundering / terrorist financing risk may be present when a Supplier is:

a. Performing certain customer-related services (examples include: on-boarding, “know your customer” screening, and the processing, monitoring, reporting or recordkeeping of financial transactions) or the delivery of data/metrics related to the foregoing activities

b. Acting as an intermediary with regard to cash or financial instruments (e.g., remote deposit capture, courier, armored car or lockbox services)

[1] *Applicable law as used in this section includes the UK Bribery Act 2010 and the US Foreign Corrupt Practices Act of 1977 and any other applicable bribery, law or regulation of any relevant country.*

Due diligence performed on the Supplier may also surface regulatory or reputational concerns related to money laundering or terrorist financing-related activities.

Where money laundering / terrorist financing risk is identified, AML and the party engaging the Supplier must work together to require that the Supplier complies with applicable AML rules and regulations and has in place reasonable and appropriate AML program, consistent with Citi requirements and supported by appropriate policies, procedures and training. The program may include such components as:

- Reporting and escalation of suspicious activity
- A "Know Your Customer" program, including a Customer Identification Program, sanctions and name screening, customer due diligence and enhanced due diligence
- Transaction monitoring
- Periodic reporting/metrics, including reporting on legal and regulatory changes and material AML program changes
- Testing and controls of AML program effectiveness, including site visits

The Contract with the Supplier must appropriately addresses AML risk by clearly defining the program to be instituted by the Supplier, including defining AML roles and responsibilities and permitting monitoring and oversight by Citi.

2.9 Human Rights in the Workplace

Equal Employment Opportunity and Fair Employment Practices; Discrimination and Harassment Policy

Citi is an equal employment opportunity employer which is committed to ensuring full compliance with the letter and spirit of all laws regarding fair employment practices and non-discrimination, and expects that all of its Suppliers shall also fully comply with all laws regarding fair employment practices and non-discrimination.

Citi policy prohibits all forms of discrimination, harassment and intimidation based on a person's race, sex, gender, pregnancy, gender identity or expression, color, creed, religion, national origin, nationality, citizenship, immigration status, age, disability, genetic information, marital status (including domestic partnerships and civil unions as defined and recognized by applicable law), sexual orientation, culture, ancestry, familial or caregiver status, military status, veteran's status, socioeconomic status, unemployment status, status as a victim of domestic violence or other basis prohibited by law.

Discrimination, harassment or intimidation that is unlawful or otherwise violates Citi policies whether committed by or against a manager, co-worker, Client, Supplier or visitor is prohibited. Retaliation against individuals for raising claims of discrimination or harassment is also prohibited. Complaints regarding such behaviour should be reported to the Citi Ethics Hotline, or the respective primary Citi business contact.

Suppliers shall recognize and respect the right of employees to freedom of association and collective bargaining and shall not infringe on employees' ability to form or join a union of their choosing.

2.10 Anti-Slavery and Human Trafficking

Citi is committed to implementing systems and controls aimed at ensuring that modern slavery and human trafficking is not taking place anywhere within its organisation or in any of its supply chains. All of Citi's Suppliers are expected to adhere to the principles set out below in this respect.

Child Labor Avoidance: child labor shall not be employed. The term "child" refers to any person under the age of 15 (or 14 where the law of the country permits), or under the age for completing compulsory education, or under the minimum age for employment in the country, whichever is the greatest. Subject to the overriding prohibition on the use of child labor, if workers under the age of 18 are employed then particular care shall be taken as to the duties that they carry out and the conditions in which they are required to work to ensure that they come to no physical, mental or other harm as a direct or indirect result of their work or working conditions.

Freely Chosen Employment: workers shall not be forced, mentally or physically coerced, bonded, indentured, or subjected to involuntary prison labor or slave trafficked or compulsory labor in any form, including forced overtime. All work must be carried out voluntarily. The principles set out below further support this commitment.

Workers must have the right to terminate their employment freely, as appropriate following a reasonable period of notice in accordance with applicable laws and collective agreements, and without the imposition of any improper penalties.

Wages, Benefits and Working Hours: Compensation should comply with all applicable wage laws, including those relating to minimum wages, overtime hours and legally mandated benefits. Employees should be able to earn fair wages, as determined by applicable local law. Work weeks should not exceed the maximum set by local law.

Workers shall not have their identity or travel permits, passports, or other official documents or any other valuable items confiscated or withheld as a condition of employment and the withholding of property shall not be used directly or indirectly to restrict workers' freedoms or to create workplace slavery.

Fees or costs associated with the recruitment of workers (including but not limited to fees related to work visas, travel costs and document processing costs) shall not be charged to workers whether directly or indirectly. Similarly, workers shall not be required to make payments which have the intent or effect of creating workplace slavery, including security payments, or be required to repay debt through work. If it is determined that fees or costs have been charged to workers related to the recruitment process or are incurred during the course of employment, the Supplier should seek to have those costs reimbursed.

Workers shall have their terms of employment or engagement set out in a written document that is easily understandable to them and which clearly sets out their rights and obligations. This written document shall include, but not be limited to, transparent terms with respect to wages, overtime pay, payment periods, working hours and rights in respect of rest breaks and holiday. Such written terms shall be provided to the worker in advance of his or her commencement of work, shall be honoured by the employer and shall meet industry standards and the minimum

requirements of applicable laws and collective agreements where the work is carried out.

Workers, their families and those closely associated with them shall not be subject to harsh or inhumane treatment including but not limited to physical punishment, physical, psychological or sexual violence or coercion, verbal abuse, harassment or intimidation. Migrant workers, their families and those closely associated with them should not be subject to discrimination in their terms or conditions of work due to their nationality.

Workers shall be free to file grievances to their employers about the employer's treatment of them and workers shall not suffer detriment, retaliation, or victimisation for having raised a grievance.

Workers shall be free to move without unreasonable restrictions and shall not be physically confined to the place of work or other employer controlled locations (for example, accommodation blocks). There shall be no requirement placed on workers that they take accommodation in employer-controlled premises except where this is necessary due to the location or nature of the work being performed.

Where it is necessary to recruit workers who are engaged via a third party, such as an employment agency, then only reputable employment agencies shall be engaged. Where workers are sourced to be employed directly, only reputable recruitment agencies shall be engaged.

2.11 Sanctions Compliance

Citi has policies, procedures and internal controls for complying with applicable U.S. and non-U.S. sanctions laws and regulations. Citi's Global Sanctions Policy requires the maintenance of processes and controls to detect, investigate, escalate, and take appropriate actions with respect to sanctions targets.

Any Supplier Personnel who are positively matched to a sanctions list entry are to be barred / removed from the Citi assignment immediately.

Actual or attempted circumvention of compliance with U.S. and local sanctions law through action or omission is strictly prohibited.

2.12 Anti-Trust and Fair Competition

In many countries, Citi is subject to complex laws designed to preserve competition among enterprises and to protect consumers from unfair business arrangements and practices. Suppliers are required to be aware of and comply with these laws at all times. The Supplier shall not at any time engage in any conduct amounting to price fixing, cartelization, abuse of a dominant position or any other illegal conduct. The Supplier shall not make, accept or discuss proposals that raise concerns about anti-competitive conduct.

2.13 Tied Business Dealings

Communicating to a Client that the price or availability of a Citi product or service is subject to the Client agreeing to purchase from or provide to Citi another product or service ("tying") is unlawful in certain instances. Suppliers are required to be aware of, and to comply with, all tying laws and any relevant Citi policy(ies) and procedures.

Suppliers may not extend credit, lease or sell property of any kind or provide any service (each, a “Tying Product”) or fix or vary the consideration for any of the foregoing, on behalf of Citi, on the condition or requirement that the customer:

a. Enter into a "tie-in arrangement"; i.e., obtain some additional credit, property or service from such bank or its affiliates, other than those related to, and usually provided in connection with a Traditional Bank Product; or

b. Enter into a “'reciprocity arrangement”; i.e., provide some additional credit, property or service to such bank or its affiliates, other than those related to, and usually provided in, connection with a Traditional Bank Product; or

c. Enter into an "exclusive dealing arrangement"; i.e., not obtain some other credit, property or service from a competitor of such bank or its affiliates, other than a condition or requirement that such bank reasonably imposes in a credit transaction to assure the soundness of the credit.

2.14 Privacy and Security of Citi’s Information

Citi is committed to protecting Citi’s Information, ensuring that such is used in full compliance with applicable laws and Citi policies and only related to Citi business. Suppliers are required to comply with all relevant laws, regulations, Citi policies and applicable Contracts concerning the protection, non-disclosure and prohibited uses of Citi Information. Without limiting the foregoing, Suppliers shall safeguard all Citi Information by ensuring that such information is used only for authorized purposes, only shared with authorized persons and is properly and securely maintained. Suppliers with access to such information or any other information which is defined as Confidential Information, Confidential Personally Identifiable Information (PII) or Restricted Information, are required to consult with the Citi Business to whom they are providing products or services with any questions regarding appropriate uses of Citi Information. See Secure Workplace Guidelines in Section 9 of these Standards.

2.15 Fraud Management

Citi is exposed to internal and external fraud risks that may cause financial loss, impact customer experience and may result in additional legal, reputational and regulatory risks, including changes to capital requirements.

Fraud risk is the dishonest use or appropriation of assets, resources, services or benefits. Fraud occurs when a person deliberately gives false information or intentionally fails to disclose information in order to deceive an owner of assets, resources, services or benefits. Fraud also occurs when dishonest acts are committed without personal gain but are intended to create a loss or risk of loss for another person or entity. This includes the intentional misrepresentation of financial condition.

Fraud risks relating to Supplier relationships can include:

- Processes and / or Controls operated by the Supplier being targeted by criminals to facilitate or commit fraud against Citi or a Citi Client;
- The Supplier misrepresenting, giving of false information or failing to disclose information either at the selection and on-boarding stage or through the ongoing lifecycle of an established relationship;

- Abuse of position by the Supplier, their employees or sub-contracted service providers to use their access to Citi data and / or processing capabilities to enable or commit fraud, which fraud will be treated as internal fraud.

Citi does not tolerate:

- Fraud committed by its staff and non-compliance with regulations;
- Fraudulent or deceptive actions committed by third parties; and
- Untimely or incomplete escalation of fraud events to Senior Management.

Citi reserves the right to investigate suspected or alleged theft, fraud or other potential criminal activity or wrongdoing and to prosecute any fraudulent or criminal behaviour to the fullest extent of the law.

All Suppliers, irrespective of the products or services provided, are required to:

a. Ensure timely reporting and referral of any potential fraud events to Citi. This includes but is not limited to, attempted, suspected, alleged or actual theft, fraud (e.g., submitting knowingly false, inaccurate or misrepresented data regarding the Supplier, billing schemes, disappearance of funds or securities, etc.), criminal activity or wrongdoing involving Citi, a Citi employee, a Citi Supplier or agent or a Citi non-employee (e.g., temporary employees and contractors).

b. Permit monitoring and oversight by Citi and its representatives and support Citi – and Law Enforcement – led investigations into potential fraudulent activity involving that Supplier in accordance with requirement 2.25 – Investigations.

Further to this, Suppliers that provide services that are inherently more exposed to fraud risk are required to:

a. Complete fraud awareness training (within 90 days of hire and annually thereafter) and train staff on specific elements of fraud risk that relate to the specific services provided to Citi;

b. Document and follow a Fraud Risk Management Program that identifies the material fraud risks relevant to the services they provide to Citi and the controls and procedures in place to mitigate these risks;

c. Monitor instances of attempted fraud and maintain effective controls to mitigate the risk of fraud on the services they provide to Citi, document procedures for controls and test the effectiveness of controls on an ongoing basis, reporting any deficiencies to the Business Activity Owner (BAO).

Suppliers with higher inherent fraud risk include, but are not limited to, those that:

a. have access to data classified as Confidential or higher (when not under Citi's direct control or supervision) that can be used to enable fraud such as access to internal accounts, financial transactions, cash transactions;

b. have connectivity to Citi networks / systems;

c. provide, support, or have access to, services and capabilities which could be targeted to commit or enable fraud, including:

    1. Identification, on-boarding or processing applications from new clients.
    2. Citi or Client Payment / Fund Transfer activities, and / or authentication of Citi clients access these services.
    3. Making, checking or fulfilling changes to Citi data or Citi-client (e.g., demographic) data.

4. Provision, servicing or authorization of transactional instruments (e.g., debit / credit cards, eWallets, chequebooks, etc.).
5. Provision or support of operational fraud management activities to Citi, relating to the prevention, detection or response to fraud events.

2.16 Continuity of Business

Citi maintains continuity of business plans to minimize financial losses and respond to market and Clients' needs when any disaster, crisis, disruption or emergency occurs. Citi must be prepared to respond to any event that may affect normal business operations. Suppliers are required to have in place appropriate continuity of business plans to ensure that any interruption regarding the products and services that the Supplier provides to Citi, are addressed and corrected within Citi's defined recovery timeframes. Suppliers are required to consult with the applicable primary Citi business contact to understand any crisis management procedures or requirements applicable to their relationship. See Continuity of Business in Section 11 of these Standards.

2.17 Privacy for Citi's Workforce

Citi seeks to protect the personal and Confidential Information it, or any of its Suppliers, collects, uses and maintains about its employees (whether on a permanent or temporary basis, including contractors), which may include, but is not limited to, medical information, government-related information (such as national or government identification and tax data) and background check information. Such information must not be transferred, processed, shared or discussed outside Citi, except where permitted or required by applicable law or regulation or pursuant to a subpoena or order issued by a court of competent jurisdiction or requested by a judicial, regulatory, administrative or legislative body of competent jurisdiction. Workforce policies and procedures for privacy and security cover Citi employees as well as other individuals whose information is provided to Citi within the context of the working relationship.

Suppliers are required to protect the personal and Confidential Information they receive about Citi's workforce and shall not transfer, store, access or otherwise process PII provided by Citi outside of the country from which it was provided without Citi's prior consent. Suppliers must comply with all Citi policies and guidelines, as well as applicable local laws and regulations, relating to security and privacy of personal and Confidential Information and ensure that such information is only shared with authorized individuals. Responses to requests for such information may be provided only as permitted by applicable Citi policy, law or regulation.

2.18 Safety in the Workplace

The safety and security of Citi's workplace is a primary concern of Citi. Suppliers are required to comply with all applicable laws and Citi policies regarding health and safety and security in the workplace. In addition, threats or acts of violence in the workplace or failure to report the aforementioned will not be tolerated.

2.19 Drug-Free Workplace

In any Citi workplace and while any Supplier Personnel is providing services or products to Citi, the misuse of controlled substances; and the sale, manufacture, distribution, possession, use within Supplier or Citi premises; or being under the influence of any intoxicating substances or non-prescribed or illegal drugs at work; or any intoxicating, illegal or non-prescribed substance abuse that renders any Supplier Personnel unfit, for duty are prohibited.

2.20 Communications, Equipment, Systems and Services

Citi's equipment, systems and services are provided for Citi business purposes only and to enable Suppliers, when authorized in advance by Citi, to perform tasks related to the products and services Suppliers provide to Citi. Accordingly, and to the extent permitted by applicable laws and regulations, Citi may monitor and record a Supplier's use of Citi equipment, systems and services at any time. Suppliers should use Citi's equipment, systems and services for authorized purposes only. Suppliers may not use Citi's equipment, systems and services unless authorized in advance by Citi and in instances in which such authorization is provided, Suppliers may not use Citi's equipment, systems and services for any inappropriate or unauthorized purpose or in a manner that would violate applicable laws, regulations or Citi's policies, standards or guidelines.

Without limiting the foregoing, use of Citi's intranet / Internet servers must be in compliance with all applicable laws and regulations and the terms of use of Citi sites and any third-party sites accessed. Citi's intranet / Internet servers may not be used for unauthorized downloading or use of any copyrighted or unlicensed material. This includes downloading music and unauthorized downloading of unlicensed software, copyrighted images, video or printed material. The Internet may not be accessed from a Citi server to view, download, store, transmit or post illegal, harassing, demeaning, offensive or inappropriate material or for any other purpose which conflicts with Citi's policies, standards and guidelines on unlawful discrimination and harassment. Copying, selling, using or distributing information, software and other forms of intellectual property in violation of intellectual property laws or license rights is prohibited.

Citi will not tolerate the use of its communications, equipment, systems and services, including e-mail services and / or intranet / Internet services, to create a hostile or offensive work environment. Suppliers must never use Citi systems to initiate, download, view, store, transmit or exchange electronic images or text of a sexual nature or containing ethnic slurs, racial epithets or any other material of a harassing, demeaning, offensive, lewd or inappropriate nature.

2.21 Safeguarding Personal, Proprietary and Internal Citi Information

a. While providing products or services for Citi and after Suppliers cease their association with Citi, Suppliers have an obligation to safeguard personal, proprietary, Internal and Confidential or higher information that they obtain or create in connection with their activities for Citi, regardless of its form. Suppliers may not bring to Citi proprietary or Confidential and higher information of any former employer or customer or use such information to aid the business of Citi,

without the prior consent of their former employer or customer and unless permitted by applicable law or regulation.

b. Suppliers will adopt, maintain and follow security practices and procedures that are sufficient to safeguard personal, proprietary and Internal information about Citi or its Clients, employees, Suppliers or distributors, regardless of its form, from any (i) unauthorized disclosure, access, use or modification; (ii) misappropriation, theft, destruction or loss; or (iii) inability to account for such Information.

c. Suppliers may only disclose, use or reproduce Citi Information as required for and related (and then only to the extent necessary), to enable the Supplier to fulfil its obligations in relation to providing products and / or services to Citi. Suppliers shall not use Citi Information or allow Citi Information to be used for any other purposes. Citi Information must not be shared or discussed outside Citi, except where expressly permitted by Citi or required by applicable law or regulation or pursuant to a subpoena or order issued by a court of competent jurisdiction or requested by a judicial, administrative or legislative body of competent jurisdiction. Unless otherwise provided by law, Suppliers shall immediately notify Citi of any subpoena, request or other attempt by any third party to obtain such information.

d. Suppliers will ensure that access to work areas and computers is properly controlled. Suppliers will not discuss sensitive matters, proprietary or Confidential Information in public places such as elevators, hallways, restaurants, restrooms and public transportation, the Internet or any other electronic media (including blogs and social networking sites).

e. Suppliers must be cautious when using mobile phones or other communication devices or messaging services. Great care must be exercised when discussing Confidential Information in open workplace areas, such as cubicles or on speaker phones.

f. Once Suppliers are no longer providing products and / or services to Citi (or sooner upon request by Citi), Suppliers must disable and terminate all means of access to any Citi system, as well as return, destroy or retain all Citi Information as directed by Citi and return all Citi property (including, but not limited to, all ID cards, keys, One Time Password (OTP) tokens (e.g., SafeWord cards).

g. Suppliers may not forward Citi Information to a home computer, personal e-mail address or to any third-party service provider or server or other non-Citi website or engage in any other unauthorized use, misappropriation or disclosure of Citi Information. Moreover, Suppliers shall not transfer, store, access or otherwise process PII provided by Citi outside of the country from which it was provided without Citi's prior consent.

h. Suppliers are responsible for ensuring compliance with all Citi policies and guidelines and the terms of any Contract relating to the safeguarding of Citi Information.

2.22 Media Interaction and Public Appearances; Use of Citi Name, Facilities or Relationships

Citi Global Public Affairs is the only department authorized to issue press releases or public statements on behalf of Citi. Suppliers may not issue any press release

which directly or indirectly identifies Citi, any Contract or arrangement between a Supplier and Citi or any products and services procured from a Supplier by Citi. Further, Suppliers may not consent to or engage in any public relations activity relating to Citi with Clients, Citi employees, other Citi Suppliers, other customers of Suppliers or any other third parties without prior written approval from their primary Citi business contact and Citi's Director of Global Public Affairs.

Suppliers may not publish or post any material in written or electronic format (including books, articles, podcasts, webcasts, blogs, website postings, photos, videos, social media or other media), make speeches, give interviews or make public appearances that mention Citi, Citi's operations, Clients, products or services, without prior written approval from their primary Citi business contact and Citi's Director of Global Public Affairs.

Whether or not in connection with the provision of services or products to Citi, Suppliers may not use Citi's proprietary indicia, trademarks, service marks, trade names, logos, symbols or brand names, without, in each case, securing the prior written consent of Citi.

Suppliers may not use Citi's name, logo or trademarks, facilities or relationships for benefit or for work outside of Citi (including on letterhead or personal websites, blogs or other social networking sites). Further, Suppliers may not make any use of Citi's name, facilities or relationships for charitable or pro bono purposes.

2.23 Insider Trading

Citi policies, as well as the laws of the United States and many other countries prohibit trading in the securities (including, but not limited to, equity securities, convertible securities, options, bonds and any stock index containing the security) of any company while in possession of material, non-public information (also known as "inside information") regarding the company. It is also illegal to "tip" or pass on material, non-public information to any other person who misuses such information by trading in securities or passing such information on further, even if no monetary benefit is received from the tippee.

Trading on or conveying material, non-public information may also breach contractual obligations assumed by Citi to, or on behalf of, Clients, as well as the provisions of the Contracts between the Supplier and Citi. Suppliers are prohibited from trading in securities based on, sharing with anyone, or using in any other way, any material non-public information about Citi, Citi's Clients or prospective Clients, or any other third party, obtained through the Supplier's work with Citi. Suppliers must keep confidential, and must not misuse, any proprietary and/or confidential information about Citi, Citi's Clients or prospective Clients, or any other third party, obtained through the Supplier's work with Citi.

Consequences for insider trading violations can be severe, including, but not limited to: termination of a Supplier's relationship with Citi (including any and all Contracts); criminal sanctions and penalties for the Supplier, for any Supplier Personnel involved and individual tippees; monetary penalties; and other damages.

2.24 Personal Investments in Citi and Other Securities

Suppliers providing services to certain Citi businesses may be subject to additional restrictions and policies regarding personal trading of securities (including Citi securities). These may include preclearance, blackout periods and reporting requirements. Affected Suppliers will be notified of and once notified must comply with, any additional restrictions that Citi applies to them.

2.25 Investigations

Suppliers are required to cooperate fully with any appropriately authorized internal or external Citi investigation, including, but not limited to, those involving ethical issues or complaints of discrimination or harassment. Suppliers may never withhold, destroy, tamper with or fail to communicate relevant information or records in connection with an investigation. In addition, Suppliers are required to maintain and safeguard the confidentiality of an investigation to the extent possible, except as otherwise provided by applicable law. Making false statements to or otherwise misleading, internal or external auditors, investigators, legal counsel, Citi representatives, regulators or other government authorities is prohibited.

2.26 Required Reporting

Unless prohibited by local laws, any Supplier employee or sub-contractor who provides services or products in a Citi workplace must notify Citi if he / she becomes subject to an arrest, summons, subpoena, arraignment, indictment or conviction for any criminal offense, including a plea of guilty or no contest and any participation in a pre-trial diversion or similar program.

2.27 Political Activities and Contributions

Political activity includes: (i) Making corporate or personal political contributions, soliciting political contributions, using Citi funds or resources (such as facilities, equipment, software or Personnel) or volunteering personal services during company time on behalf of a candidate campaigning for a public office, a political party committee or a political committee; (ii) lobbying or engaging in any outreach to public officials, whether directly or through third parties, including attempts to influence legislation and, depending on the jurisdiction, may include attempts to influence agency rulemaking or the awarding of government contracts; or (iii) seeking, accepting or holding any political office associated with a government, including any government board, commission or other similar organization.

A variety of laws regulate political activities of Citi and its Suppliers. Any political activity by Suppliers that is not in compliance with relevant law or regulation is prohibited.

In addition, no political activity may be undertaken or conducted by any Supplier on behalf of (or purportedly on behalf of) Citi without prior written authorization of Citi's Global Government Affairs office. Citi will never reimburse a Supplier for personal or corporate political contributions of any kind.

2.28 Charitable Contributions

Charitable contributions may not be given on behalf of Citi by a Supplier or requested by or from a Citi employee, Client, government official or other Citi business partner as a condition of or in order to influence a business decision (i.e., no "*quid pro quo*").

2.29 Corporate Opportunities

Suppliers owe a duty to Citi to advance its legitimate interests when the opportunity to do so arises. Suppliers may not take for their own use a potential corporate opportunity for Citi that is discovered in the course of the Supplier's engagement with Citi or through the use of Citi property, information or position; nor may Suppliers compete against Citi.

2.30 Related-Party Business Dealings

Suppliers must notify Citi of any business relationship or proposed business transaction Citi may have with any company in which the Supplier or a related party has a direct or indirect interest, from which the Supplier or a related party may derive a benefit or where a related party is employed, if such a relationship or transaction might give rise to the appearance of a conflict of interest.

2.31 Reporting Concerns

Maintaining ethical standards is critical to Citi to maintain world-class business standards. If you have any questions regarding the best course of action in a particular situation, or if you reasonably suspect or become aware of a possible violation of a law, regulation, Citi policy, Citi Code of Conduct or ethical standard, you must report it by promptly contacting your Citi Third Party Officer, Citi business contact, the Citi Ethics Office, or any of the other contacts listed in the Citi Code of Conduct.

The Citi Ethics Office may be reached by:

- Calling the Citi Ethics Hotline, a toll-free number (available 24 hours per day, seven days per week in multiple languages) at: 1-866 ETHIC 99 (1-866-384-4299)
- Or dial your country access code and 866-384-4299
- Or 1-212-559-5842 (direct or collect)
- E-mailing ethicsconcern@citi.com
- Website submission at: http://www.citigroup.com/citi/investor/ethics_hotline.html
- Mailing to: Citi Ethics Office
One Court Square
Long Island City, NY 11101
U.S.A.
- Faxing to: 1-212-793-1347

All contacts and investigations are treated as confidentially as possible, consistent with the need to investigate and address the matter, and subject to applicable laws and regulations.

Complaints may be made anonymously to the extent permitted by applicable laws and regulations. However, you must understand that if you do choose to remain anonymous, Citi may be unable to obtain the additional information needed to investigate or address your concern.

If you raise an ethical issue and you do not believe it has been addressed, you should raise it with another of the contacts listed in the Citi Code of Conduct.

3 ACCESSIBILITY AND DIVERSITY

Citi encourages the utilization of Diverse Suppliers and is committed to assist Diverse Suppliers in their growth and development on a long-term basis. In addition, Citi encourages its Suppliers to develop and utilize Diverse Suppliers as sub-contractors, when applicable. Additional information about Citi's Supplier Diversity Program can be found on the Citi Supplier Diversity website:

http://www.citigroup.com/citi/citizen/people/diversity/index.htm.

The Supplier shall remain at all times compliant and procure the compliance of each of its agents, sub-contractors, employees and workers, with all anti-discrimination and equal opportunities legislation applicable to each of its Personnel (including disabled Personnel) and to Deliverables as per Citi's instructions (as may be agreed in any agreement or transactional documents raised thereunder).

Supplier shall use all reasonable endeavours to itself adhere, and procure that each of its sub-contractors adheres, to the current relevant codes of practice in relation to employment of disabled persons and to the delivery of services that is compatible with equal opportunity legislation (as contained in the Americans with Disabilities Act 1990, the Telecommunications Act 1996 and in the United Kingdom the Equality Act 2010 or similar).

Furthermore, Supplier shall use all reasonable endeavours to ensure that any contribution it makes to any services (defined as any goods, services, facilities, privileges, advantages, or accommodations that Citi provides to members of the public, whether they are provided in Citi's physical locations or online) delivered by or on behalf of Citi to the public comply with applicable ADA Title III requirements, including compliance with digital standards as outlined by the World Wide Web Consortium's (W3C) Web Content Accessibility Guidelines (WCAG) 2.0 AA and with the 2010 ADA Standards for Accessible Design. Any adverse findings regarding this compliance will be properly remediated in a timely manner, so as to not harm Citi's business operations.

4 ENVIRONMENTAL SUSTAINABILITY

As reflected in our commitment to the environment, Citi recognizes that environmental sustainability is integral to good business practices and production of world-class products. Citi also recognizes that climate change is a major economic, social and environmental challenge globally. Citi has set global goals to address climate change across our business and driving environmental and social progress in our supply chain is fundamental to our sustainability performance.

Citi has set a target to source 100% of our energy use from renewable sources by 2020. We are also working with our clients to provide innovative solutions as they strive to reduce their emissions and monitor progress. We encourage our Suppliers to join us in similar sustainability efforts. Our target for Suppliers is to continuously maintain:

4.1 An Environmental Policy

We encourage all Suppliers to have an effective environmental policy and to endeavor to achieve this policy using the best available techniques; to implement this policy at all levels throughout the company; and to include a commitment to continual improvement in environmental performance, energy efficiency, and waste reduction. Suppliers are expected to follow sustainable practices that promote a high level of environmental and social performance, manage risk, and help us assess the Greenhouse Gas (GHG) emissions in supply chain.

4.2 Life Cycle Analysis/Implementation

We encourage utilization of life cycle analysis to minimize a service or product's environmental impact during its entire life cycle by considering the use of recycled material, energy consumption during service delivery, manufacturing and use, material identification, disassembly, choice of material, etc. Operational practices that reduce any environmental burden associated with our activities are promoted. Innovative developments in products and services that offer environmental and social benefits are encouraged.

4.3 Pollution Prevention and Recycling

We encourage reduction or elimination of waste of all types, including water and energy, at the source, or by practices such as modifying production, maintenance and facility processes, materials substitution, conservation, recycling and re-using materials. Water and solid waste generated from operations, industrial processes and sanitation facilities should be monitored, controlled and treated as required prior to discharge or disposal, and recycled to maximum effect.

IT Hardware and Electronic Equipment (examples such as Telecomm including servers, personal computing, mobile devices, tablets, desktops) provided by Suppliers must have high energy efficiency (energy star or other equivalent labels) and their material composition must be from renewable or recycled materials and / or have high levels of ease of reuse and recycling associated with them, such as vendor trade-in programs, design for disassembly, etc., and Suppliers must provide validation on correct disposal with certified processes, such as e-steward and / or R2 standards e-waste recyclers if recycled or refurbished. In addition, Suppliers will

be required to furnish proof that they have complied, where applicable, with reporting requirements related to sourcing of conflict minerals, where such requirements are imposed on them by local legislation.

4.4 Conservation and Resource Utilization Reductions

To the extent possible, and with continual improvement, we expect implementation of conservation and resource utilization reduction programs to conserve resources and eliminate wastes of all types.

4.5 Hazardous Material Safety

Chemical and other materials posing a hazard if released to the environment should be identified and managed to ensure safe handling, movement, storage, recycling or reuse and disposal.

4.6 Air Quality and Emissions

We expect our Suppliers to implement a reasonable and comprehensive Air Quality Program. Emissions of carbon should be monitored and minimized; emissions of volatile organic chemicals, aerosols, corrosives, particulates, ozone depleting chemicals and combustion by-products generated from operations should be characterized, monitored, minimized, controlled and treated as required prior to discharge.

Travel and logistics Suppliers will be required to disclose their reported GHG Emissions (Scope 1 & 2) and stated corporate targets (if applicable).

4.7 Sustainable Forests

Following Citi's Sustainable Forestry Standard (part of the Environmental and Social Policy Framework), Citi recognizes forests provide essential goods and services to both local and global communities and markets. Citi is connected with, and committed to, efforts to sustain healthy forest systems. Our Suppliers should take steps to ensure that they do not buy from or contract with any company knowingly engaged in illegal logging.

In addition, Suppliers are expected to track their sourcing of paper and paper-based products and report their progress on their sourcing and use of sustainable paper and paper-based products on an annual basis through the Supplier Corporate Responsibility Questionnaire (CRQ). To do so, Citi expects Suppliers to only source paper and paper-based products with proven certification by one of the following initiatives and certifications: Sustainable Forestry Initiative (SFI), Forest Stewardship Council (FSC) standard, and Programme for the Endorsement of Forest Certification (PEFC).

4.8 Management Systems

We encourage our Suppliers to institute targeted ethical, social and environmental programs with effective management systems (e.g., International Organization for Standardization (ISO), Eco-Management and Audit Scheme (EMAS), etc.) that utilize the best available techniques and practices to achieve sustainability and corporate social responsibility at all levels, and to strive to continuously improve their

performance. We encourage Suppliers to clearly communicate the contents of these Standards, and their own internal standards that meet or exceed these principles, to their employees and contractors, and to offer adequate training, and utilize self-evaluation programs to assure conformity with standards and applicable laws.

4.9 Implementation

We encourage all our new and existing Suppliers to aspire to these guidelines and endeavor to make continual improvements. As the intent of these Standards is to increase ethical business practices and social and environmental sustainability throughout the supply chain, we will encourage our Suppliers to require their next-tier Suppliers to acknowledge and implement parallel best practices and standards of conduct. We further encourage and challenge our Suppliers and their Suppliers to offer and innovate new and better products and services reflecting ethical practices and sustainability attributes for Citi purchase at cost competitive pricing.

5 SUPPLIER RELATIONSHIP AND CONTRACT COMPLIANCE

a. Suppliers and potential Suppliers must cooperate with their primary Citi business contact to ensure that a Non-Disclosure Agreement (NDA) is executed (or that an agreement including similar confidentiality and non-disclosure obligations for the Supplier is in place) with Citi prior to any discussions or exchange of any Citi Confidential Information between Citi and Supplier.

b. Suppliers must not commence performance of any services or provide any products to Citi unless a Contract has been fully negotiated and executed between Citi and the Supplier or a purchase order (PO) has been issued to the Supplier by Citi.

c. Suppliers must keep their primary Citi business contact aware of any changes in the Supplier's key management team and / or respective contact information.

d. Suppliers must support Citi's efforts to perform appropriate and required ongoing Supplier management activities and cooperate as necessary, including Information Security Assessments and information about customer complaints and their resolution, if required. Additional due diligence is performed for Suppliers designated as Outsource Service Providers (OSPs). Suppliers must provide necessary support to Citi businesses to perform additional due diligence, when applicable. (For example, see Section 10 Information Security of these Standards).

e. Suppliers who engage in consumer facing activities are required to maintain procedures for complaint / concern handling as defined in Section 12. Consumer facing activities include those in which a Supplier, acting on behalf of or at the direction of Citi, interacts directly with a Citi consumer or related party. Suppliers must apply Citi's definition of complaints / concerns and implement processes supporting Complaint / Concern Identification (definition), acknowledgement, capture, escalation, research (investigation) and response consistent with Section 12. Citi Supplier Oversight is responsible for communicating and overseeing third party implementation of complaint / concern requirements, monitoring adherence to the requirements and establishing effective analysis and reporting. Suppliers are required to provide Citi with Complaint / Concern detail and data on a regular basis, and in a format consistent with Citi tracking requirements. Supplier exceptions need to be approved within applicable Complaint Advisory Committees.

f. Suppliers with access to systems, facilities and information classified as Confidential Information or higher must support Citi's requests to provide information for identification purposes.

g. Unless otherwise agreed by Citi in writing, a Supplier may not use a sub-contractor to fulfil Supplier's obligations to Citi. If permitted to use a sub-contractor, (a) Supplier must confirm that the sub-contractor can comply with all obligations applicable to the Supplier; (b) the Supplier must ensure that the proposed sub-contractor will comply with all obligations applicable to the Supplier; and (c) the Supplier will remain responsible to Citi for overall performance and any noncompliance by the sub-contractor with Supplier's Contract with Citi.

h. Any approval of the sub-contractor must be documented in a written acknowledgement signed by the Supplier that reaffirms the Supplier's obligations

in subsections (b) and (c) of the preceding paragraph (g), depending on the criticality or risk level of the proposed sub-contractor activity, as Citi deems necessary. The exact form and text of the written Acknowledgement may be changed based on the underlying Contract with the Supplier and any precise terms deemed necessary and approved by Citi. Please work with the primary Citi business contact to document approval utilizing the appropriate Consent Form.

Acknowledgement of Supplier in Connection With Use of Subcontractor
Acknowledgement of Supplier in Connection With Use of Designated Subcontractors

i. Citi may require Suppliers to provide the most recent three (3) years audited year-end financial statements and upon request the most recent financial interim statements. Supplier may further be asked to provide written consent to allow Citi to provide the Supplier's financial statements to a third party service provider engaged by Citi for the purpose of translation or performing a Financial Evaluation.

j. Citi may request information to confirm and / or documentation to validate that Supplier has satisfied any required service and quality levels, documentation to assess the adequacy of the Supplier's Continuity of Business (CoB) program and practices (see Section 11 of these Standards), and / or compliance with any of the terms of its Contract.

k. Suppliers must ensure that at all times it is in full compliance with any and all applicable Export laws and shall provide reasonable and necessary information to Citi if the services and products provided by Suppliers to Citi involve or require the sharing of any technical data, computer software or any product (or any part thereof), process or service that is the direct product of any such technical data or computer software outside of the United States or with any individuals who are not citizens or residents of the United States. In addition, depending on the nature of the products and services, Citi may require Suppliers to identify export classification for such products and services. Additionally, Suppliers will comply with all applicable export laws outside of the United States, as well as applicable local laws and regulations and will notify Citi of any specific requirements with respect to Citi's use of the products and services outside of the United States.

l. Supplier will not assign to Citi or retain on assignment to provide services to Citi, any Personnel that Supplier knows, suspects or has reason to believe has been convicted of, pled guilty to or participated in a pretrial diversion for, a crime involving dishonesty, breach of trust, money laundering or any other type of crime whether or not related to the services. Citi may require Suppliers to complete and successfully pass a criminal background check (that may include fingerprinting), as a condition of providing services for Citi or provide satisfactory written evidence that the criminal background check has been performed and the results thereof, upon Citi's request, when permitted by local law.

m. Supplier must maintain and effectively administer comprehensive policies and procedures for conducting background checks for its Personnel who are natural persons and are intended to be assigned to provide services for Citi to the extent permitted by, and in accordance with, applicable laws and any applicable collective bargaining agreement. Those policies and procedures must meet Citi's Standards for background screening, including, without limitation, reviewing Personnel's employment history, criminal convictions and pre-employment drug testing. Citi

may, at any time, request information to validate that Supplier has conducted all background screening in accordance with Citi Standards and all applicable local laws and regulations.

n. Citi's expectations of Suppliers in conducting background screening on their Personnel are defined in Section 13 Global Background Screening Standards in these Standards.

o. Citi may require Supplier to procure and ensure that Suppliers' Personnel read, acknowledge and accept their compliance with Citi policies, including those related to security and privacy, workplace policies and other policies, procedures and guidelines intended to ensure compliance with applicable law or regulatory requirements.

p. Supplier must comply with all applicable immigration laws and regulations of the countries in which its Personnel perform any service for Citi. Supplier must fulfill employment eligibility verification requirements and ensure that its Personnel are authorized to work in the countries to which they are assigned. Supplier must ensure that its Personnel hold the appropriate visa classification for the types of services they are performing for Citi, and that neither Supplier nor its Personnel violate in any other manner the immigration laws and regulations of the countries in which they are performing services for Citi. Upon discovery of any noncompliance, by itself or its Personnel, Supplier must immediately notify Citi and take appropriate corrective action.

q. Supplier will sign and provide, and as applicable ensure that its Personnel will sign and provide, to Citi on-boarding documents as required by Citi before assigning Supplier Personnel. Supplier will comply with all Citi policies and processes, including requests for work verification letters and invitation letters (with potential sanctions at business level if vendor does not comply). Supplier agrees that, if any of its Personnel seeking to enter any country to provide, or purporting to provide, services to Citi are refused a visa or are refused admission by immigration officials, Supplier will immediately provide notice of such refusal to Citi and will provide copies of all available documents related to such refusal.

6 EXPENSES

Citi will only reimburse reasonable business related expenses that have been pre-approved in writing by Citi and have been incurred by the Supplier in connection with the provision of products and services to Citi and in accordance with the terms of the applicable Contract and supported by receipts. These should be properly documented and invoiced to Citi in accordance with Citi invoicing requirements. For clarification, an expense for which the Supplier seeks reimbursement from Citi is subject to prior written approval of Citi by a Citi employee who has been granted the appropriate level of delegated authority to approve the expense. Supplier expenses may not be incurred by a Citi employee on behalf of a Supplier. Any invoice submitted to Citi for expense reimbursement for a valid and approved expense item(s) must include (in addition to all other invoicing requirements):

- The business purpose of the expense;
- The amount and description of the expense;
- Place and date of the expense;
- The project name / description for which the Supplier is providing services;
- The names and business relationship of the Citi representative requesting the service(s) for which such expenses were incurred; and
- Purchase Order number, where applicable.

Payment terms that have been established between Citi and Supplier in the applicable Contract also apply for expense reimbursements.

For information on reimbursable business expenses, please contact your primary Citi business contact. All reimbursable travel must be booked using Citi's Travel Management Company (TMC), where applicable. Full travel itineraries and invoices must be submitted with the reimbursement claim and approved by appropriate business sponsor and / or primary Citi business contact. Non-compliant requests will not be reimbursed. Supplier may not submit for reimbursement the non-compliant amounts.

The following are excerpts with appropriate modifications from the Reimbursable Business Expenses section of the Citi Expense Management Policy and are applicable to Supplier and its Personnel with respect to booking travel using Travel Management Company (TMC) through to reimbursement. For information on reimbursable expenses, please contact your primary Citi business contact.

I. **Travel Related Non-Reimbursable Expenses:** Supplier and its Personnel shall not, under any circumstances, be reimbursed for any non-reimbursable expense items.

II. **Travel Related Reimbursable Expenses:** Subject in all cases to Supplier's and its Personnel's compliance with the terms of the applicable services agreement, the following items may be eligible for reimbursement to the extent incurred on travel for Citi business:

6.1 General

Travel reservations must be made through a Citi Travel Management Company (TMC), where available. For contact information to the local Citi TMC, please contact your primary Citi business contact. When using the Citi TMC, Suppliers and their Personnel must provide the TMC a Citi non-employee ID (NEMS ID), where

applicable or the Citi employee ID (GEID) of their Citi "sponsor" (the Citi employee with whom they are conducting business).

a. Bookings include:
    1. Hotels
    2. Rental vehicles
    3. Point-to-point air travel
    4. Multi-leg air travel within the U.S.
    5. Eligible train travel, unless the TMC instructs the traveller that the booking needs to be made directly with the carrier

All travel must be categorized as client / revenue generating or non-client / non-revenue generating:

a. Citi Client / Citi Revenue Generating is defined as expenses directly associated with client related or revenue generating activities.
b. Non Citi-Client / Non-Citi-Revenue Generating is defined as business critical activities not associated with revenue generating activities including legal, supervisory, regulatory and Continuity of Business activities.

Supplier and its Personnel are strongly encouraged to purchase air tickets and book hotels, at least 7 days in advance of departure date.

Supplier and its Personnel may not make or modify travel arrangements for personal gain.

a. Supplier and its Personnel may not downgrade a class of service (e.g., business class to economy class) in order to use the savings for personal use or pay more than the discounted fare to obtain an additional mileage bonus or other benefit.

Citi's Global Travel Program cannot be used by a Supplier and its Personnel for personal travel.

Commutation expenses are not reimbursable.

Ground transportation costs are reimbursable for business related purposes only:

a. Toll tags, discount token purchases, unlimited train and bus passes are not reimbursable, unless used exclusively for Citi business-related travel.

Spousal travel is not reimbursable.

Internet access charges incurred while travelling are reimbursable when Internet access is required exclusively for Citi-related business purposes.

If eligible bookings are NOT booked through the Travel Management Company where available, Supplier and its Personnel will not be reimbursed. Explanation of such must be detailed in reimbursement request.

Emergency travel changes due to severe weather (e.g., blizzard), Continuity of Business invoked or reported travel incident (e.g., airport disruption or closing) where the Supplier and its Personnel could not contact the Travel Management Company can be made directly with the commercial air carrier, hotel, rental agency or the eligible train travel rail provider.

6.2 Commercial Air Travel

Supplier and its Personnel must book the Lowest Logical Airfare, with a Citi preferred airline.

a. The TMC will provide information on flights within the applicable travel window and from this, will offer the Lowest Logical Airfare.
b. Travel window for international flights is two hours and for domestic and intra-EMEA flights is one hour on either side of requested departure time.
c. Supplier and its Personnel are not required to make a stop when a non-stop flight on a Citi preferred airline is available.
d. The TMC may also provide information on airfares from alternate airports. The option to depart from an alternate airport is recommended when airfares are lower and business objectives are not compromised.
e. Citi Client related travel requiring the Supplier to take the same flight or class of service as the Client or where the Lowest Logical Airfare arrival time is not conducive to critical client meeting time must be booked using the TMC.

Airline travel must be Coach / Economy class. Business Class (or one class above Coach / Economy Class) is permitted for:

a. Intra-EMEA: All flights above 1,200 miles (one way)
b. All other flights above 2,100 miles (one way)

If Supplier and its Personnel wish to upgrade to a higher class of service than the permitted class of service, the cost of the upgrade is not reimbursable.

Supplier and its Personnel must use eTickets, where available.

Supplier and its Personnel must cancel any reservation that will not be used prior to the scheduled departure time to ensure a refund is processed.

Supplier and its Personnel may not choose higher airfares for personal gain (e.g., frequent flyer miles, frequent flyer status or companion tickets). Supplier and its Personnel may retain frequent flyer miles if there is no incremental cost to Citi.

Chartered flights are non-reimbursable.

Reimbursement:

a. If flights are booked through the Travel Management Company (TMC)
    1. Supplier and its Personnel will be fully reimbursed if the Lowest Logical Airfare was accepted, otherwise the cost in excess of this is non-reimbursable
    2. Supplier and its Personnel must submit both the TMC invoice and itinerary including Citi in-policy / out-of-policy remarks to be reimbursed
    3. In the event changes are made and the resulting fare is higher, the revised travel agency issued invoice that indicates the new fare and any additional changes must be attached to any claim for reimbursement.
b. If flights are NOT booked through the Travel Management Company where required, Supplier and its Personnel will not be reimbursed.

6.3 Ground Transportation

Ground transportation includes the use of motor vehicles for business purposes including car rental, personal vehicles, trains, buses and private cars or taxi services.

a. Rental vehicles:

1. The approved rental vehicle classes are Standard and below.
    i. A full size car or Sport Utility Vehicle (SUV) may be rented only when four or more passengers will use the vehicle.
    ii. Specialty / luxury vehicles are not reimbursable.
2. Fines for traffic or parking violations are not reimbursable.
3. Fuel costs for rental vehicles are reimbursable.

b. Personal vehicles:

1. Use of personal vehicles for Citi business travel is reimbursable based upon the incremental distance travelled over normal commuting. Fuel costs are not reimbursable.
2. A Supplier and its Personnel who uses his / her vehicle for business travel will be reimbursed in accordance with local tax laws based upon documentation of distance travelled, dates of travel origin and destination and an appropriate business reason.
    i. Parking, tolls and mileage are reimbursable
    ii. Fines for traffic or parking violations are not reimbursable
    iii. Expenses associated with theft or damage of a Supplier and its Personnel's vehicle (including insurance deductible payment) while on Citi business are not reimbursable.
    iv. Parking costs and daily commuting expenses to / from work as part of normal commute are not reimbursable.

c. Private cars:

1. When public transportation is not available or appropriate, taxi, Approved Private Car Service or reimbursable private car service must be used, where available. For a list of Approved Private Car Service and reimbursable private car service providers, please contact your primary Citi business contact.
    i. The cost is reimbursable only when used for business related purposes; e.g., transportation to / from airport when traveling on an approved business trip, transportation to / from a client meeting or transportation home post late night work after 10:00 p.m. (all locations).
    ii. Supplier and its Personnel requiring transportation between Citi offices should use public transportation or Citi operated Shuttle Services where available.
    iii. Supplier and its Personnel should utilize complimentary transfers to / from the airport when provided by an airline as part of the airfare. Supplier and its Personnel will be notified where available.
    iv. Supplier and its Personnel in major cities may use a non-approved car company for service that originates or terminates outside the municipal limits.

v. Charges for stops are non-reimbursable except for ride-sharing purposes when used for business travel. The expense reimbursement request must include departure / arrival location, date, type of car, business purpose and names of attendees.

vi. Car phone, personal rides and no show fees are non-reimbursable.

vii. Tips are not reimbursable when using an Approved Private Car Service.

viii. Surge pricing and on-demand luxury vehicles are not reimbursable when utilizing reimbursable private car service. All exceptions must be approved by the Citi Chief Financial Officer (CFO).

ix. On-demand Black Car vehicle classes are not reimbursable when utilizing a reimbursable private car service, unless Citi does not have an approved private Car Service Supplier in that location. Use of reimbursable private car service Black Car vehicles is permitted where Citi does not have preferred ground transportation Suppliers. All exceptions for reimbursable private car service vehicle classes must be approved by the Citi CFO. When using reimbursable private car service, you are encouraged to use the lowest cost vehicle option available. Tips may be reimbursed when using a reimbursable private car service, where allowed.

x. Supplier and its Personnel are strongly encouraged to use alternative ground transportation during reimbursable private car High Demand periods.

xi. Supplier and its Personnel must submit receipts in accordance with the Expense Management acceptable forms of receipt documentation in order to obtain reimbursement.

xii. A SUV may be utilized only when three or more passengers will use the vehicle.

2. Use of six passenger or stretch limousines is prohibited.

d. Train travel:

1. Eligible train travel must be booked through the Travel Management Company, unless the Travel Management Company instructs the traveller that the booking needs to be made directly with the carrier.
2. All train travel is to be coach, second-class or lowest available express services.
   i. First-class train travel, including Club and Custom class, is permitted when used instead of a more expensive, in-policy airline ticket
   ii. Use of first-class train travel requires that a written explanation be attached to Supplier's or its Personnel's reimbursement request.

e. Shuttle Service:

Shuttle Services provides Supplier's Personnel with transportation to / from selected Citi office buildings for business meetings. Citi ID or a valid visitor pass must be shown when boarding the Shuttle Service.

6.4 Hotels

Supplier and its Personnel must book all hotels, extended stay hotels and serviced apartments through the Citi Travel Management Company.

Client related travel requiring the Supplier or its Personnel to stay at the same hotel as the Client must be booked through the Travel Management Company and does not require exception approval.

Supplier and its Personnel must book the lowest available Citi negotiated rate at a Citi Preferred Hotel most convenient to where they need to conduct Citi business.

In cities without a Citi Preferred Hotel, Supplier and its Personnel will be directed by the Citi Travel Management Company to an approved hotel and rate.

Where Supplier's Personnel requires hotel stays of > 5 nights, they must stay in accommodation identified as Citi preferred extended stay hotels or serviced apartments where available.

Extended stay hotels and serviced apartments which cannot be reserved through the Citi Travel Management Company must be booked through the Citi Global Travel Department.

Supplier and its Personnel must cancel any reservation that will not be used in accordance with the hotel no-penalty cancellation policy. Supplier and its Personnel must obtain a cancellation number.

a. Reimbursement

1. If hotels are booked through the Citi Travel Management Company
   i. Supplier or its Personnel will be fully reimbursed if the approved hotel and rate was chosen. Any exceeding cost will not be reimbursed.
   ii. In addition to the itemized hotel bill, Supplier or its Personnel must submit both the Citi Travel Management Company invoice and itinerary including policy remarks for hotel stays to Enterprise Supply Chain (ESC) to be reimbursed.
   iii. Supplier and its Personnel must submit the Extended Stay and Serviced Apartment Approval Form to Citi's ESC for accommodation booked by the Citi Travel Management Company.
2. Where required, if hotels are NOT booked through the Citi Travel Management Company, Supplier or its Personnel will not be reimbursed. The only reimbursable circumstances for hotel stays not booked through the Citi Travel Management Company are as follows:
   i. Client related travel requiring a Supplier to stay at a hotel booked directly by the Client or external firm handling travel logistics for Client related travel
   ii. Attending external seminars, conferences, association meetings or conventions that offer special group or discounted rates at the meeting site or at hotels convenient to the site does not need to be booked through the Travel Management Company. A copy of the conference registration must be submitted with the reimbursement request as proof of attendance.

6.5 Meals

a. Travel Meals

1. Reimbursement of travel meals are permitted when one or more individuals are traveling and incur a meal.
2. Travel meal daily limits are defined by Citi, and are used to determine the maximum reimbursement per person per day (i.e., the daily limit should be multiplied by the number of attendees) and based on the location in which the travel meal expenses are incurred. For the travel meal daily limits, please contact your primary Citi business contact.
3. The averaging of travel meal expenses among days is not permitted.
4. Any amounts exceeding the travel meal daily limits will not be reimbursed.

7 GIFTS AND ENTERTAINMENT

In general, Suppliers may not provide gifts or convey anything of value (including entertainment) to Citi employees, where doing so would create an actual or apparent conflict of interest, compromise the employee's integrity or judgment or otherwise improperly influence the employee's decision making or cause the employee to act contrary to his / her duties. Without limiting the foregoing, cash gifts or their equivalent (e.g., gift cards or vouchers) are not permitted under any circumstances and Suppliers must not provide non-cash Business Gifts[2] exceeding, in aggregate, U.S. $100 per person per calendar year to a Citi employee. Any Citi's employee's acceptance of Business Gifts is subject to pre-approval per the Citi Gifts and Entertainment Standard, and may be subject to additional limits under specific Citi business, regional and / or legal entity policies.

When a Supplier provides Business Entertainment (e.g., an invitation to a meal, social, sporting, cultural or other comparable event) to a Citi employee, the Supplier must be in attendance at the event and the entertainment must be appropriate, customary and reasonable, not lavish or excessively frequent and clearly not meant to influence Citi business.

Supplier may not, on behalf of Citi or purportedly on behalf of Citi, provide gifts or entertainment, or anything of any value, to any person outside Citi.

[2] A "Business Gift" is any item of value (other than Business Entertainment) given or received by a Citi employee in connection with Citi's business or the business of the external party, generally excluding items valued at USD $25 or less.

8 RECORDS MANAGEMENT

Citi requires that all Suppliers with custody of Citi Information work with their Business Activity Owner (BAO) or primary Citi business contact to (i) classify Information as Records or Transitory for Citi's records management purposes, (ii) classify Records in accordance with Citi's Master Record Catalogue (MRC), (iii) retain Information based on the retention requirements and (iv) absent Record Holds, appropriately dispose of Information at the end of the Information Lifecycle.

Supplier must work with their primary Citi business contact or BAO to ensure the Records Inventory identifies records according to Citi record codes in the MRC and is updated at least annually. Supplier has the obligation to abide by the Records Management requirements communicated by the BAO. Records that have met the retention obligation listed in the MRC and not on a Record Hold, must be destroyed according to Citi Information Security Standards within 12 months of eligibility. Records and information identified by Citi as subject to the European Union's General Data Protection Regulation (GDPR) must be destroyed within 6 months of eligibility. Supplier must suspend destruction or alteration of Citi Information when notified of a Record Hold. Transitory Information must be destroyed no longer than two years after its last use, provided it is not subject to a Record Hold. Supplier shall check with their primary Citi business contact or the BAO in the event of any uncertainty.

Suppliers must not dispose of any Citi Information, irrespective of its classification (e.g., Confidential, non-Confidential) without their primary Citi business contact or BAO approval, which must include confirmation that no active Record Holds apply to the Information due for disposal. Retention requirements and all other information handling requirements shall survive termination or expiration of the Contract, unless explicitly agreed to otherwise.

Suppliers shall maintain documentation listing all Supplier Personnel responsible for overseeing management of Citi Information in Supplier custody and hold periodic meetings with their primary Citi business contact or Records Management Officer (RMO) to review and update contact names, procedural details, roles and responsibilities and the Supplier Record Inventory.

9 SECURE WORKPLACE GUIDELINES

Item	Requirements
Citi Information (electronic and hard copy documentation)	Lock up and secure Citi Information after normal work hours and anytime Supplier is away from designated workspace.
Personal Property (wallet, planner, cell phone, etc.) and Computing Devices (Laptops, PDAs, Blackberrys, Cell phones, etc.)	Personal possessions and computing devices must never be left unattended. Citi is not responsible for loss of Supplier's personal possessions or computing devices.
Desktop Personal Computers (PCs) and Laptops	PCs and laptops used to access or view any Citi Information must be secured by screen saver passwords after a period of inactivity. Whenever a Supplier steps away from designated workspace they must lock the PC and / or laptop with CTRL + ALT + DEL and select "Lock Computer". If a Supplier is using a laptop to view Citi Information, Supplier must ensure that such laptop is secured via cable or security locks to the base unit during work hours and locked securely away after normal work hours.
Logoff of PCs	Supplier must logout and shutdown all PCs being used by the Supplier before the Supplier leaves unless business needs require that it is on. If a Supplier workstation is left on, the Supplier must make sure that it is locked and the monitor is turned off.
Storage Areas	Areas under desks and tops of cabinets must not be used to store excessive personal items or material that may contribute to a potential fire or physical hazard.
Lock It Up	File cabinets and drawers must be locked after normal work hours.
Open Office Areas	Open office areas must not be used as file server / mini-data centers unless specifically designed for such use and documented with Citi.
Printers, Photocopiers and Fax trays	All sensitive paper must be cleared from printers, photocopiers and fax trays.
Private Offices / Conference Rooms	All policy guidelines apply regardless of whether the Supplier is occupying an office. Note that private offices and conference rooms are not necessarily secure, even when locked, because service Personnel has access to them.
Disposal	Dispose of Citi Information that is no longer required (follow specific retention schedules). Documents must be shredded or placed in a secure / locked recycle bin. Magnetic media must be disposed of securely after proper erase procedures have been followed.

10 INFORMATION SECURITY (IS)

10.1 Overview

This Section provides requirements for Citi's Suppliers, who store, process, manage or access Citi Information and / or host Citi applications, regarding the information protection controls that are expected by Citi to ensure that information is protected in accordance with applicable legal and regulatory requirements and the highest industry standards (for example, ISO / IEC 27002) in the locations where Citi and its Suppliers do business.

These Standards merely set minimum requirements. If local laws, regulations or relevant industry standards establish a higher standard than provided here, Suppliers must comply with such laws, regulations or standards. In addition, Suppliers may be required to incorporate additional information security practices and procedures as part of their compliance with other Citi policies and terms and conditions of a Contract.

If a Supplier decides to implement additional security practices or detailed procedures for information security, the Supplier must ensure that those practices and procedures do not conflict with the minimum controls defined in this section.

10.2 Information Security Policy

a. Information security policy document

1. Suppliers must have documented information security policies and standards. Ownership for these documents must be assigned to a Supplier officer or team whose responsibilities include annual reviews and updates (hereafter the 'Owners').
2. Supplier must have a documented process that describes roles, responsibilities and governance for their information security policies, procedures and standards.

b. Review of the information security policy

Supplier's information security policies and standards must be reviewed by Supplier's management, on an annual basis at a minimum, for organizational appropriateness, consistency with the state of technology, the most recent industry standards, compliance with legal and regulatory requirements and Citi's required standards.

10.3 Organizational Information Security

a. Management commitment to information security / assessments

1. Suppliers, who will host a Citi-branded Internet-facing application and / or have access to Citi Information with an information classification of Confidential or higher, are subject to Citi's Third Party Information Security Assessment Process (TPISA) for assessment of Supplier's policies, procedures and controls regarding compliance with Citi Standards and any legal and / or regulatory requirements (applicable to either Citi or Supplier) that pertain to information security. The assessment will consist of security questionnaires requiring responses from Supplier with evidences and visits

to locations where Citi's Confidential or higher Information may be stored, processed, managed or accessed by the third party to meet the business needs of Citi and its clients. Should the findings of a TPISA disclose or indicate security problems or concerns, Citi will document findings in a notice to Supplier and work with Supplier to identify means for correcting the problems. Suppliers must expeditiously make the necessary corrections or add necessary compensating controls to address Citi's concerns to reasonable satisfaction; and in any event within 180 days for High Risk issues, within 240 days for Medium Risk issues and prior to the next assessment for Low Risk issues.

2. Citi may independently collect and review cyber threat and similar data related to Supplier and its systems and assets, based on public data sources, in connection with the assessment of Supplier's information security and cyber risks, and may share the results of such reviews with Supplier from time to time. Supplier acknowledges that Citi has no responsibility or liability for any inaccuracies, limitations or failures of such reviews to identify threats or risks to Supplier's systems or assets, and Citi disclaims any implied warranties or duties in connection with such activities.
3. Supplier must regularly perform assessments of its business operations and related controls against the Supplier's information security standards, policies and procedures.
4. The periodic assessments must include, at a minimum:
    i. Assessment of the processes that the Supplier uses to ensure compliance with IS policy and standards.
    ii. Assessment of supporting resources, such as applications and infrastructure used by the Supplier and IS processes used by the Supplier's sub-contractors (if applicable) that support their business operations, or, in the alternative, to allow Citi to conduct such assessments. Compliance is required in the event a third party signs a new or renews an existing contract with a sub-contractor that accesses, processes, manages or disposes of Citi Information classified as Confidential or higher.
    iii. Assessment of all activities and (sensitive) data that are of inherent high internal fraud risk. At a minimum, assessment must cover funds transfers processes, block removals on post-no-debit / credit, dormant / inactive accounts, whereabouts unknown accounts, servicing friends & family accounts, write-offs, card issuance, destruction and stock reconciliations, cash and original documentation handling, procurement procedures, off office hours' activities, trading amendments such as cancels and corrects, and client demographic data, payee data and PINs.
5. Issues that have been identified as a result of any Information Security risk assessment must be documented and tracked to closure.
6. If Supplier's Information Security management function is relocated across country borders, the Supplier must obtain Citi's documented approval.

7. If Supplier acquires a new entity, the Supplier must complete an assessment of the acquired entity for compliance with these Standards in accordance with the requirements in this section.
8. The Supplier must not outsource Security management functions including, but not limited to, firewall management, security configuration management, patch management or Information Security Administration (ISA) functions, for systems used to store, process and / or transmit Citi Information unless approved in writing in advance by Citi.
9. If Supplier hosts a website that contains Citi Information or is Citi branded, periodic vulnerability assessments of that website must be performed and any material issues identified during the assessment must be remediated in a timely manner.
10. If connectivity to servers and / or Information Systems on the Citi internal network is required, then Supplier is required to notify their primary Citi business contact so that the current connectivity process can be followed.
11. The Supplier must promptly notify the appropriate Citi contact of any unauthorized access or acquisition or loss or corruption or deletion of Citi Information or any other compromise to Information Systems used to store, process and / or transmit Citi Information.
12. The Supplier must ensure that all high risk activity and changes to sensitive data have audit trails that enable specification of what individual performed what activity or changed what data.
13. The Supplier must ensure that all sensitive data is masked on screen and on paper (including e.g., monitoring, exception and regulatory, and other reports).
14. The Supplier must restrict printing, recording or copying of sensitive data, including by 'own devices'.

10.4 External Parties

a. Identification of risks related to external parties

1. Supplier must notify Citi, in writing, of any intent to use sub-contractors to support operations involving Citi Information and must not use any sub-contractor unless and until consented to in writing by Citi. If Citi consents to the involvement of sub-contractors:
    i. A Non-Disclosure Agreement (NDA) or an agreement containing appropriate confidentiality obligations on the part of such potential sub-contractor must be executed by Supplier with each potential sub-contractor prior to discussions about or the exchange of, any Citi Information and such an agreement must be in force for so long as any Citi Information is made available to such potential sub-contractor.
    ii. The sub-contractor is to be screened against the U.S. sanctions and applicable non-U.S. sanctions list, and jurisdiction subject to sanctions.
2. Supplier must ensure appropriate security of Citi's Information and Information Systems that are accessed, processed, disposed or managed by sub-contractors.

i. Supplier must ensure that the security of Citi Information and Information Systems are not compromised by the introduction of the products or services provided by a sub-contractor.

ii. Supplier must periodically review the information security controls of sub-contractors that host a Citi-branded Internet-facing application or that have been given access to Citi Information.

iii. Supplier must annually evaluate its relationship with those sub-contractors that meet the criteria specified above to determine if a review of their security controls is required.

3. When access to Citi Information needs to be provided to third parties, or sub-contractors, outside of the Supplier's facilities and management oversight, information security requirements, as appropriate, must be addressed in a documented agreement between the Supplier and the additional party that includes:

   i. The right to periodically perform an information security assessment, or similar audit substantially, consistent with the one that Citi may conduct on the Supplier, and an obligation to have, upon request, any material issues found in the assessment remediated or establish the corresponding compensating controls.

   ii. A requirement that the party promptly notifies the Supplier when there has been any unauthorized access or acquisition of Citi Information or any compromise to Information Systems used to store, process or transmit Citi Information.

   iii. Requirements that the party performs all reasonable efforts to return or destroy all Citi Information at an agreed point in time during or at the end of the agreement.

   iv. Requirement that the sub-contractor and the sub-contractor’s employees used for Citi assignments are subject to screening against the U.S. sanctions and applicable non-U.S. sanctions lists, and jurisdictions subject to sanctions.

   v. A requirement that sub-contractors limit access to Citi Information to only those sub-contractor employees who have a need for such access in order to provide the underlying services to the Supplier.

   vi. The obligation of the sub-contractor to use the information only for the purpose of providing the services to the Supplier and not to disclose Information to any of its sub-contractors or third parties without written permission from Citi, unless required by law.

   vii. The right to terminate the agreement, with notice to the party, if the security requirements of Citi change and the third party does not agree to such changes.

4. Agreements with parties, who require access to servers and Information Systems on Citi’s internal network, must, in addition to the requirements above, include the right for Citi to revoke access or interrupt the connection between Citi and the third party’s systems.

5. Each use of External Cloud Provider involving Confidential or higher information or serving as a production system must be approved by Citi

prior to going live and annually thereafter.

10.5 Asset Management

a. Inventory of assets

1. Supplier must ensure that an Inventory is maintained of all applications and hardware under its control that are used to store, process and / or transmit Citi Information.
2. Supplier must ensure that an Inventory of Citi Information Assets is maintained under its control in accordance with a process used to appropriately maintain the accuracy and completeness of that inventory.
3. If Supplier uses Functional IDs on Production / Continuity of Business (CoB) Information Systems, the IDs must be maintained in an inventory(s), capturing the key attributes.
4. Supplier must ensure that of Critical Data Assets under their control is maintained.

b. Protection of assets

1. Supplier must be responsible for protecting all Citi Information under its control.
2. All Functional IDs on Production / CoB Information Systems where Citi Information resides must not be created unless an owner is designated and have an owner at all times. The Functional ID owner may nominate a delegate(s) to assist in the fulfillment of the responsibilities associated with the ownership of the ID. The ID owner is responsible for compliance with all Functional ID requirements.

c. Access and Acceptable Use of Assets

1. Supplier must ensure accountability of its Users' activity in a manner consistent with industry practice.
2. User access to personal external Internet e-mail accounts must be restricted from the Supplier's global network where Citi Information resides.

d. Information classification

1. Citi classifies information per the following Information Classification:
   - Restricted
   - Confidential
   - Internal
   - Public
2. Authentication is a separate classification with its own requirements as defined within these Standards. It is completely independent of other Information Classifications.
3. PII Attribute: Personally identifiable Information (PII) can be categorized in any data classification. Appropriate controls must be applied commensurate to the risk level of PII within those classifications.

e. Information labelling, handling and storage

1. Based upon the classification of Citi Information, the Supplier must specify the level of security required to protect such information and ensure that

sufficient controls are in place, along with any heightened or modified levels that Citi may subsequently set.

2. Citi Information must be stored on:
    i. Citi managed devices or within Citi managed applications that provide comparable controls including data protection and policy enforcement.
    ii. Third Party managed devices that are subject to a Contract between the Third Party and Citi that contains confidentiality provisions consistent with Citi policies and standards.
3. Only information classified by Citi as Public may be stored on Supplier Personnel-owned devices (e.g., home computers, personal digital assistants, mobile Internet and e-mail applications).

10.6 Physical and Environmental Security

a. Fire Safety

1. Supplier must comply with applicable legal and regulatory requirements governing physical security and the establishment of a safe work environment, including local fire codes.
2. Supplier must utilize a fire detection, alarm and suppression system(s). The system(s) must be inspected and tested annually.

b. Physical Security

1. Citi Information must be stored in secure areas with controls that restrict access to only authorized Personnel.
2. The Supplier must have a documented and auditable physical access system in place.
3. The Supplier must utilize a combination of security alarm / intrusion systems that include a security alarm monitored by a third party, security guards and video surveillance as appropriate for the environment and services provided.
4. The Supplier must have a documented visitor policy that includes the requirement for all visitors to provide verifiable identification upon arrival, sign-in and sign-out.

10.7 Communications and Operations Management

a. Document operating procedures

Supplier must have a documented Secure System Development Life Cycle (S-SDLC) in place, in adherence to Citi's minimum standards, if the Supplier provides software development services to Citi.

b. Change management

Supplier must have a documented Change Management Process in place.

c. Segregation of duties

1. Supplier must put processes in place to ensure that no individual person, can perform any two business functions or two of the IT functions, or two of the Controlled Information System functions with persistent access for the same activity, change, Information System or transaction without authorization or detection unless adequate compensating controls are present to mitigate the risk. Currently, the following are the only recognized exceptions:

i. A User may initiate or approve a real transaction and still participate in testing of new requirements for the same Citi Information System in a non-production environment.

ii. A User with the Develop function may provide production support, but persistent access to the Citi Information System can only be granted if the access is limited to read or view only and does not include access to Confidential Restricted data.

2. A person with the Develop or Certify function who needs to provide break / fix support utilizing the Implement function must use temporary privileged access to the Controlled Information System.
3. A person who needs to update production data outside of application controls must use temporary privileged access.
4. A person who needs to view data containing Confidential PII or Restricted / Restricted PII data outside of application controls must use temporary privileged access.
5. Individuals performing the Develop or Certify function must not modify or install operating system or database infrastructure software in Controlled Information Systems

d. Separation of development, test and operational facilities

Where applicable, Supplier must ensure that the Development, Test and Production environments are all physically and / or logically separated from one another.

e. Service delivery

Supplier must have documented agreements in place with sub-contractors who have access to Citi Information that fully meet Citi Standards, along with mechanisms in place to ensure compliance by any such sub-contractor(s) with such agreements and these Standards.

f. Capacity Management

Supplier must have a documented Capacity Management process in place that meets relevant industry standards.

g. System acceptance

Supplier must have documented Project Scope Management and System Acceptance processes in place that meets relevant industry standards.

h. Controls against malicious code

Supplier must ensure that the necessary precautions are taken to prevent and detect the introduction of any malicious code (e.g., viruses, worms, Trojan Horse viruses, adware, spyware, etc.) and must implement preventive, detective and recovery controls to protect against malicious code.

Supplier must:

1. Implement, update and maintain technology for anti-virus and anti-spyware on all personal computers and technology for anti-virus on all Local Area Network (LAN) servers, mail servers and other devices that store, process and / or transmit Citi Information.
2. Establish an appropriate blocking strategy on the network perimeter.

3. Implement technical and process controls to ensure that Personnel do not access external Internet email accounts or non-business related website from the Supplier network
4. Implement perimeter Infrastructure that provides the capability for blocking access to Internet sites that are deemed to be non-business related or present an information security risk.

i. Controls against mobile code

Suppliers must ensure that necessary precautions are taken to appropriately control the use of Mobile Code. Where the use of Mobile Code is authorized, the configuration must, at a minimum, meet all industry standards and contractual obligations to Citi, ensure that the authorized Mobile Code operates according to a clearly defined and documented security policy and prevent unauthorized Mobile Code from executing.

For Mobile Code that can affect the underlying operating system or platform (i.e., outside the "sandbox"), Supplier must ensure the following:

1. Mobile Code published by Supplier must be signed by a Citi-approved Certificate Authority and the lifecycle of the certificate must be managed by the Supplier to address expiration or rotation of the certificate.
2. Signed Mobile Code with expired certificates must be removed from production.

j. Network controls

1. Supplier networks used to store, process and / or transmit Citi Information must be protected from threats and security must be maintained for the Information Systems using the network. This includes information in transit across the network.
2. Information with a Citi Information Classification of Confidential or higher must not be persistently stored on a system in an Internet-facing Demilitarized Zone (DMZ).
3. With regard to networks used to store, process and / or transmit Citi Information, Supplier must ensure that:
    i. Only Wireless Local Area Networks (WLANs) or other wireless device solutions that include reasonable controls to prohibit unauthorized access (PEAP-TLS, EAP-TTLS, etc.) may be connected to networks that contain Citi Information.
    ii. All external IP connections to the Supplier global network are protected by a Supplier managed firewall.
    iii. A real-time Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) is in place that monitors and protects Internet connections to their network where Citi Information is stored, processed or transmitted.
    iv. All Citi branded Internet applications and services hosted at Supplier sites must have Citi-approved anti-DDoS (Distributed Denial of Service) services or comparable controls validated by Citi.
    v. External firewalls must be configured with a default "deny all" rule. Firewall rules must be configured based on the least privilege principle.

k. Management of removable media

1. Supplier must protect Citi Information regardless of the media upon which it is maintained. This Standard applies, but is not limited to, the following types of media upon which information is contained: card, cassette, compact disk (CD), check stock, diskette or other removable storage device, hard copy output, magnetic disk, magnetic tape, microfilm, microfiche, optical disk or paper document.
2. The default setting for access to portable media / storage devices for the systems where Citi Information is stored must be no access. If exceptions are granted and thus read-write access is permitted, the data must be encrypted on the portable media device.

l. Disposal of media

When Citi Information with a Citi classification of Confidential or higher is eligible for disposal in accordance with instructions provided by Citi (i.e., at the point at which the information is no longer required by or useful to Citi, plus any additional period of retention required by law, regulation and / or Citi policies), the Supplier must destroy such Information in a manner that renders it unusable and unrecoverable.

This applies to Citi Information stored in both non-electronic formats (e.g., paper, microfilm, microfiche) and electronic formats, including but not limited to, digital media / storage devices, file shares, SharePoint sites, and embedded in office systems such as printers, copiers or fax machines.

m. Information handling procedures

1. Supplier must always protect Citi Information from unauthorized access, modification or deletion.
2. Citi Information placed upon Electronic Transportable Media (ETM) must be securely transferred and delivery must be confirmed. Supplier must confirm that the ETM was received by the intended recipient on the expected date of delivery and continue to follow up with the intended recipient until such time that the delivery is confirmed. If confirmation of receipt is not received by the expected date of delivery, Supplier must notify Citi.

n. Electronic messaging

Instant messaging, peer-to-peer networks or other Internet collaborative tools may not be used to transmit or store Citi Information outside the Supplier network or from networks that contain Citi Information, unless appropriate encryption is in place for all Citi data per Section 10.9c (Policy on the use of cryptographic controls).

o. Electronic commerce

Information Systems used to store, process and / or transmit Citi Information, that use dynamic passwords or digital certificates must use authentication services which are acknowledged by industry analysts to meet all minimum criteria for information security to validate the credentials.

p. Online transactions

1. Where applicable, Supplier must have Information Systems that use dynamic passwords or digital certificates to validate the credentials.
2. All Certificates' lifetimes must be replaced at least once every two years.
3. For all Internet facing websites and point-to-point communications between Citi and Supplier, Extended Validation (EV) certificates must be used.
4. All Supplier applications storing, processing or transmitting Citi Information must:
    i. Have an Authentication method based on the types of Data / Functions accessed; Supplier should contact its primary business contact for current requirements.
    ii. Perform a Multifactor Authentication (MFA) compliance assessment; Supplier should contact its primary Citi business contact for current requirements.
    iii. Implement an online Suspicious Activity Detection (SAD) solution; Supplier should contact its primary Citi business contact for current requirements.

q. Audit logging

Supplier must ensure that all Controlled Information Systems used to store, process and / or transmit Citi Information use audit trails at an infrastructure or application level to log the following items:

1. Infrastructure security relevant actions for the associated platform must be logged.
2. All system alarms associated with a firewall or IDS / IPS generated Security Event must be logged.
3. All attempted violations of system security (e.g., failed User login attempts) must be logged.
4. All significant events relating to financial transactions and Citi Information which specifically include the following items must be logged:
    i. Updates to financial transactions
    ii. Updates to Confidential PII data
    iii. Updates to Restricted data
    iv. Updates to Authentication data
5. Session artifacts (IP address at minimum or other pertinent information), such as unique device ID must be captured, if technically feasible, and logged for Citi facing applications (websites and mobile applications) to support fraud investigations. These artifacts must be captured for Citi transactions and for Citi account opening activity. Information must be captured in such a way that the session artifact can be linked to the transaction or account opening.
6. Significant ISA events must be logged specifically including the following items:
    i. User creation
    ii. Modification of User access rights

iii. Deletion, creation and modification of roles / profiles on the Controlled Information System.
iv. Password reset
v. Changes to system security configuration

7. All interactive activity of privileged Functional IDs must be logged.
8. Security logs must contain at least the following information regardless of the system generating the log, unless it is not technically feasible:
   i. Date and time of event (UTC formatted time)
   ii. User ID of person performing the action
   iii. Type of event
   iv. Asset or resource name affected
   v. Type of access (delete, modify, etc.)
   vi. Success or failure of event
   vii. Source (terminal, port, location, IP, Host Name, etc.)

r. Monitoring system use

1. The following events must be captured, logged and reviewed either directly or through an automated review process:
   i. All system alarms associated with a firewall or IDS / IPS generated Security Event must be reviewed.
2. Significant ISA events as noted in Section 10.7q (Audit logging) with the exception of:
   i. Removal of entitlements from user, role or profile.
   ii. Where Information Security Administration activity is executed by an automated workflow / fulfillment system that has end-to-end integrity controls.
3. All updates to critical resources as identified in the secure standard build.
4. All interactive activity performed by privileged Functional IDs or temporary ID must be reviewed.

s. Protection of log information

1. Supplier must ensure that access controls are in place to preserve the integrity of audit trails:
   i. During initiation and shutdown
   ii. In storage and during transmission
2. To prevent unauthorized modifications to the audit logs, Supplier must ensure that logs cannot be overwritten or modified by the system users whose activity they track.
3. Supplier must define retention period for log data that complies with the Citi Records Management Policy and all applicable legal and regulatory requirements and maintain and comply with such retention requirements.

t. Clock Synchronization

The clocks of all relevant information processing systems within an organization or security domain must be synchronized with an accurate time source.

10.8 Access Control

a. Access control policy

1. Supplier must implement access controls that:
   i. Are fully documented
   ii. Are auditable
   iii. Grant least privilege
2. Supplier must protect all Controlled Information Systems used to store, process and / or transmit Citi Information from unauthorized access and must secure them using security products, functions or processes commensurate with the IS Risk Ratings of the Information Systems and the applicable Information Classification.
3. Supplier is responsible for the access rights of Users in its organization.
4. Temporary Privileged Access to Controlled Information Systems must follow a documented password / account release process that:
   i. Requires the requester to either be on a pre-approved authorized users list or have an approval at the time of use.
   ii. Requires documented justification in a change / problem ticket before access is granted.
   iii. Includes an independent review of the activity performed with the access.
   iv. Includes a process to revoke / remove the access after a pre-defined period of time of no more than 24 hours.
   v. Allows, for production and post-implementation stabilization such as after a major upgrade or break / fix resolution, access to be extended up to seven calendar days.

b. User registration

1. Supplier must ensure that no users can gain access for themselves to a Controlled Information System used to store, process and / or transmit Citi Information without approval from their manager or manager's designee.
2. Persistent Privileged Access may be granted to a user on a Controlled Information System used to store, process and / or transmit Citi Information only when all of the following conditions are met:
   i. The justification for persistent access is documented as part of the approval.
   ii. The User's manager and the information owner / delegate of the Controlled Information System approve the access.
3. All new Functional IDs or changes to an existing Functional ID on Production / CoB Information Systems must be approved by the ID owner / delegate and the owner of the Information System on which it resides, as part of the ID creation and / or modification Process.
4. The Functional ID owner / delegate of any privileged Functional ID must approve additions to the authorized user list, if it exists.

c. Privilege management

1. Supplier must implement access controls that ensure Users are given only those privileges and entitlements necessary to perform their function.
2. Supplier must implement a Process to ensure that all default access capabilities are removed, disabled or protected to prevent their unauthorized use.
3. The direct login to a privileged Functional ID must be granted through a temporary privileged access Process.

d. Review of user access rights

1. Supplier must implement a documented Process to review, verify and delete unnecessary User entitlements to Controlled Information Systems used to store, process and / or transmit Citi Information.
   i. Supplier must review all User entitlements at least semi-annually and remove any unnecessary access by notifying the prior to each individual employee exiting.
   ii. Users must not review or approve their own entitlements or the entitlements of an individual who delegated review responsibility to them.
   iii. The entitlements for all privileged non-fixed Functional IDs on Production / CoB Information Systems must be reviewed annually by the ID owner / delegate.
2. For each individual employee supporting Citi, immediately notify the Citi Manager of exit date for the removal of Citi entitlements.

e. Password use

1. User static passwords must never be shared, made known to others or written down.
2. Privileged interactive Functional ID passwords on Production / CoB Information Systems must not be shared.

f. Clear desk and clear screen policy

Supplier Personnel are required to protect Citi Information in all forms, including physical information used or stored at their workspace. Suppliers are required to communicate this requirement to all of its staff at least annually through IS awareness.

g. User authentication for external connections

1. Remote access to Information Systems used to store, process and / or transmit Citi Information must be protected from unauthorized use.
2. If Supplier permits individuals to access its network remotely, the Supplier must ensure that remote access is secured by either token-based or certificate-based authentication using standard remote access technologies (i.e., VPN, Citrix, etc.).

h. Equipment identification in networks

1. Only Supplier devices (i.e., hardware, including, but not limited to: desktops, laptops, removable data storage media) that comply with these Standards

and that are authorized by the Supplier may access the Supplier Network where Citi information is stored, processed or transmitted.

2. Only Supplier devices (i.e., hardware, including, but not limited to: desktops, laptops, removable data storage media) that comply with these Standards and authorized by Citi may have access to the Citi network.

i. Segregation in networks

1. Supplier must ensure that all Information Systems and applications that are used to store, process and / or transmit Citi Information and are accessible via the Internet, are only accessed via the Supplier's demilitarized zone (DMZ).
2. During an emergency event, Supplier must be able to filter access between portions of the network to reduce the impact from network Security Events (e.g., port filtering during a virus outbreak).
3. Remote Access and Host Security must implement group-based access controls (e.g., staff, sub-contractors) to limit access to network resources in the Supplier network. At the host level, access control can be done at the group or individual level.

j. Secure log-on procedures

Login IDs associated with a static password must be locked out after a maximum of six consecutive failed login attempts.

1. Functional IDs are exempt from the requirement of locking out login IDs after the prescribed number of failed login attempts.
2. Locked out user login IDs must be re-enabled through an industry standard reset service or another authorized function. A banner text, when supported by the operating system or application, must be displayed at all network entry points where a User initially signs on or is authenticated.

k. User identification and authentication

1. All Supplier controlled Information Systems must authenticate the identity of users or systems accessing these platforms prior to initiating a session or transaction where Citi Information may be accessed.
2. All users must be:
    i. Uniquely identified or mapped to the technology platform by a User ID.
    ii. Authenticated to the technology platform using a method of authentication, Supplier should contact its primary business contact for current approved methods.
    All use of shared authentication infrastructure (e.g., Single Sign-on, Reduced Sign-on and other shared authentication services) must be in accordance with the authentication requirements; Supplier should contact its primary business contact for current approved methods.
    iii. Functional ID owners must ensure processes are implemented which clearly demonstrate accountability for interactive access.

l. Password management system

1. User static passwords must never be displayed on the screen in clear text.

2. Interactive Privileged Functional ID passwords must not be hardcoded in clear text.
3. For Active Directory, Siteminder and LDAP, static passwords (other than PINS) must contain a minimum of eight (8) characters, which must contain both letters and numbers, and be case sensitive.
4. For all other environments, Static passwords (other than PINs) must consist of a minimum of six characters, which must contain both letters and numbers and, if technically feasible, be case sensitive.
5. PINs may be used as the sole method of authentication to access Information Systems only if the PINs are necessary to meet physical device constraints (e.g., keypad, telephone, smart card).
6. All static passwords must be changed every 90 calendar days at a minimum. Same static password should not be used within at least the last six (6) changes. Static passwords for Functional IDs are exempt from this requirement. Note also:
    i. Functional IDs can be set to not expire.
    ii. All authentication systems must enforce a login inactivity/non-use control that should not exceed 100 days if technically feasible (Functional IDs and Customer login IDs are exempt from this requirement). Disabled logins may be re-enabled by the user or another authorized function.
    iii. The authentication Process must ensure that the same password was not used within at least the last six changes.

m. Use of system utilities

Supplier must ensure that the use of Utility Programs that are capable of overriding system and application controls (e.g., booting up from peripheral devices) are restricted and controlled.

n. Session time-out

1. Re-authentication or login must occur for all Users of a Controlled Information System used to store, process and / or transmit Citi Information.
2. Users must be required to re-authenticate after a period of inactivity not exceeding 30 minutes. Activity includes any input to the endpoint (mouse, keyboard, touch screen, etc.). Where enforcement is provided by the password protected screen saver, Application / Single Sign On enforcement is not required.

o. Mobile computing and communications

1. All Supplier-managed laptops and all desktop machines used to store, process and / or transmit Citi Information, using remote access where there is local storage / processing of information with a Citi Information Classification of Confidential or Restricted, must be encrypted using an encryption tool that meets industry standards.
2. Supplier-managed machines must have a personal firewall active when directly connected (i.e., not through a Supplier-managed firewall or proxy) to the Internet.

3. Any Citi Mobile Applications must be signed and published to mobile marketplaces (e.g., iTunes) by Citi.

p. Teleworking

1. All connectivity to the Citi network must use Citi's approved remote connectivity solutions.
2. Non-Citi managed devices using remote access must only use a Web-based portal solution that provides no storage off of the Citi network.
3. Citi managed devices must be regularly connected to the Citi network to enable the devices to receive and install regular updates of software, software patches (including those to protect against viruses) and virus signature updates. Such updates must be promptly applied.

10.9 Information Systems Acquisition, Development and Maintenance

a. Security requirements analysis and specification

1. Supplier must incorporate information security procedures into its processes and procedures for the selection, development and implementation of applications, products and services.
2. Supplier must have a secure build procedure for all systems where Citi Information is stored, processed and / or transmitted.
3. The secure build procedure must include tools to support automated configuration checking of the security / standard build settings at the time of production deployment.

b. Input data validation

1. Suppliers must have controls in place to protect against online security threats (i.e., cross-site scripting, SQL injection, etc.)
2. Input validation must be implemented for all Internet and intranet applications.

c. Policy on the use of cryptographic controls

The following table describes the encryption requirements. For transmissions involving information with a Citi Information Classification of Confidential PII or Restricted data, encryption must be performed on an application-to-application / server-to-server basis. When information is stored or transmitted by a Supplier-hosted application, the Supplier is responsible for compliance.

Function/Data	Encrypt in Transmission**	Encrypt in Persistent Storage
Restricted Data	All Environments	All Environments
Restricted PII data	All Environments	All Environments
Authentication Data	All Environments[1]	All Environments [1]
Confidential PII Data	• Non-Citi Managed Infrastructure[2] • Identity Verification Data[3] • Existing Applications [4] • New Applications [4] • External Email	• Non-Citi Managed Infrastructure[2] • Identity Verification Data[3]
Confidential Data	• Non-Citi Managed Infrastructure[2] • External Email	• Non-Citi Managed Infrastructure[2]
Remote Access	All Environments	N/A

1. *Authentication data: one-time use, dynamic, or pre-expired passwords do not need to be encrypted during transmission and / or in storage.*

2. *Third Parties who store or process Confidential or higher information must either meet the encryption requirements or provide comparable controls validated by an IS assessment and accepted by the Business. (Such information must be encrypted in transit to and from the Third Party when sent electronically).*

3. *Confidential PII data used for identity verification (examples include but are not limited to transaction history, credit information, address, etc.) is not subject to the additional encryption requirements for authentication data.*

4. *For all new and existing internal or external applications that went into production on or after 2012, Confidential PII must be encrypted using EATDS-approved end-to-end encryption software or tools*

*** The transmission of data can take many forms including, but not limited to Electronic File Transfers (e.g., FTP, NDM), Web Traffic, E-Mail, and Inter-Process Communications (e.g., application to application) using various protocols*

In addition to the above encryption requirement, additional criteria have been defined for the following environments:

1. **External Individual Email:** Encryption requirement for individual emails containing Citi Information with a Citi Information Classification of Confidential (non-PII) between Citi and Supplier, where the Supplier is not permitted to use Citi-approved end-to-end encryption software or tools per regulation and / or Supplier policy, may be fully met through transport encryption (e.g., gateway-to-gateway encryption via Transport Layer Security (TLS)).
2. **Private networks:** Private networks that are independently regulated by a recognized authority and are considered a Financial Services Industry standard for transacting business between licensed or accredited counterparties (e.g., SWIFT or a central bank) may be considered exempt

from the Confidential PII in transit encryption requirement until the time that those networks provide the necessary infrastructure to fully support encrypted transmissions.

3. **External Parties:** When Citi data classified as Confidential or higher is provided by the Supplier to an external party (sub-contractor) that external party must either meet the requirements of these encryption requirements or provide comparable controls validated by an IS assessment and accepted by the Supplier. (Such information must be encrypted in transit to and from the sub-contractor when sent electronically.)
4. **Voice and Fax:** Information with a Citi Information classification of Confidential or higher sent over fax or discussed on voice calls (including Voice Over IP [VOIP]) may be sent unencrypted. If required, Supplier should develop specific procedures and guidance to protect Confidential or higher information sent via these channels.

d. Key management

1. Industry standard cryptographic algorithms and minimum key lengths must be used to implement encryption.
2. Wireless networks must be encrypted with industry standard encryption algorithms.
3. Suppliers utilizing any form of cryptographic mechanism must use industry standard key management tools and techniques.

e. Control of operational software

1. Supplier must ensure that:
    i. Only operating systems and software that are currently supported by an industry accepted commercial provider or have an active and appropriate release of patches and configuration updates available to address security issues are used.
    ii. A documented process is implemented that specifies the time periods within which all approved security patches and configurations are applied.
2. Supplier must ensure that, irrespective of any separate maintenance agreement between Supplier and Citi, software developed for Citi and governed under a license agreement:
    i. Does not require use of versions of non-supported software with known vulnerabilities.
    ii. Is updated and patched as required in a timely manner.

f. Protection of test data

1. It is not permitted to put Citi Information classification of Confidential or higher on a Non-Production System without the express written authorization of Citi.
2. Where Supplier has received written permission to store these data types, the Supplier must irreversibly redact data using tool/methods that meet industry standards so it is no longer sensitive or implement the same controls as a production system.

g. Change control procedures

1. Supplier must ensure that configuration changes to firewalls, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) go through the Supplier's Change Management Process.
2. Access granted to production through temporary IDs must be logged and monitored for tracking changes made to the environment.
3. For Controlled Information Systems containing customer Information with a Citi classification of Confidential or higher or an IS Risk component value for "Integrity", or an "Availability" of High, logs captured according to Section 10.7q (Audit logging) must be reviewed by the Supplier on a sampled basis. The reviews may be based on an appropriate risk-based sampling methodology.
4. The review must validate that changes to be completed as part of the temporary privileged access were made as intended.

h. Information Leakage

Supplier must have a documented Secure Coding Standard in place that prevents information leakage, including:

1. Detailed system information (e.g., server type and technology).
2. Stack traces and exception errors that reveal directory tree structure and the underlying database type.

i. Management of technical vulnerabilities

If Supplier is accessing, storing or processing Citi data on applications or infrastructure that it manages, then it must ensure that vulnerability assessments are performed and any vulnerability issues are remediated in accordance with Citi's System Security Testing Standard.

10.10 Information Security Incident Management

a. Reporting information security events

1. Supplier should report any Security Incident that compromises or endangers the confidentiality, integrity, or availability of Citi data, or data for which Citi has a custodial obligation, or the information systems housing said data; regardless of how, who (Citi personnel or a Citi vendor or partner), or where (on or off Citi property) the incident occurred.

   Examples of Information Security Incidents (SIRTs) include:

   i. Misusing of Citi information, in any media or format
   ii. Unauthorized access (physical or electronic) to Citi Information
   iii. Communication of sensitive Citi Information to unauthorized individuals
   iv. Unauthorized modification of data
   v. Sharing Passwords
   vi. Computer intrusion (e.g., malware attacks, attacks on Citi's Internet sites)
   vii. Distributed Denial of service (DDoS) attacks
   viii. Data destruction
   ix. Loss of Citi data in any medium

2. Suppliers must immediately notify the appropriate Citi Business when there has been any unauthorized access or acquisition of Citi Information, or any compromise to Information Systems used to store, process or transmit Citi information.
3. Any suspicious activity must be acted upon immediately

b. Reporting security weaknesses

Supplier must have a Process to ensure that Application and Infrastructure Vulnerabilities that result in a compromise of Citi Information Assets are reported to Citi immediately.

c. Responsibilities and procedures

Supplier must ensure an effective approach is applied to the management of IS incidents impacting Citi Information. Supplier must maintain processes to respond to IS Incidents and notify Citi within an agreed upon period of time, any incident with a likelihood of high Severity rating that may involve a significant risk to Citigroup customers or the franchise, including where the incident: (i) involves a significant number of customers; (ii) involves a large dollar amount; (iii) is likely to be the subject of press coverage; or (iv) is likely to result in the non-routine notification of a regulator should be reported within 2 hours and all other security incident should be reported within not to exceed 24 hours of a detection of a IS Threat or IS Vulnerability on a 24-hour by 7-day per week basis. This includes, but is not limited to, IS Incidents, IS Threats or IS Vulnerabilities generated from IDS/IPS/Network Behavior Anomaly Detection (NBAD).

11 CONTINUITY OF BUSINESS

11.1 Overview

Citi maintains business continuity plans to minimize financial losses and respond to market and Clients' needs in the event of any manmade or natural disaster, crisis, disruption or emergency. Citi must be prepared to respond to any event that may affect normal business operations.

All Citi Suppliers are required to have in place documented business continuity plans to ensure that any interruption with respect to the products and services the Supplier provides to Citi are addressed and corrected within Citi's defined recovery timeframes.

If applicable, continuity plans must contain the following elements or else indicate that the element is not applicable: Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO), recovery procedures, manual workarounds to be employed when technology is not available, recovery location and resource requirements, recovery location staffing plan (including business and technology recovery staff), Citi contact information (e.g., contacts, contracted service levels), sub-contractor information, application information, procedures for returning to the primary work location, call lists, calling procedures and offsite storage lists.

Supplier business continuity plans must be updated at least annually.

All Citi Suppliers are required to provide the primary Citi business contact and Citi Senior Country Operating Officer with operating procedures to be carried out in the event that business resumption and disaster recovery plans are implemented.

11.2 Recovery Resources

Suppliers' business continuity plans must provide alternate resources capable of delivering all products and services to Citi in the event that the Supplier's primary locations become disabled. Recovery resources must be located in geographically separate locations from the primary locations with sufficient separation to minimize or eliminate the threat that the same disaster event may affect both the primary and recovery locations. Recovery resources are not limited to Information Systems, but include all resources required for continued delivery of products and services to Citi and may include staff, buildings, business equipment, data centers, data and voice networks and transportation services.

11.3 Recovery Service Levels

Supplier's business continuity must meet established levels of service in order to be effective for Citi. At minimum, Supplier's business continuity plan shall establish specific values for the following variables:

a. Recovery Time Objective

Duration in hours between the time of a service disruption and the restoration of products and services

b. Recovery Point Objective

The point in time in the past, stated in hours, to which data must be recovered after a business interruption. It is the maximum targeted period in which data

might be lost from an IT service due to a major incident. The RPO is only a measure of the maximum time period in which data might be lost if there is a Major Incident affecting an IT Service. It is not a direct measure of how much data might be lost, for example, to the end of previous day's processing.

c. Recovery Capacity

The volume, quantity or speed of delivery for the Supplier's products and services, expressed as a percentage of normal delivery of products and services.

d. Recovery Duration

It is the maximum duration, in days, that the Supplier is capable of sustaining operations whilst in recovery mode.

11.4 Disaster Recovery Plan

Citi's Continuity of Business Policy requires Suppliers that are included in a Citi Business Recovery Plan to have a contingency plan and related processes or controls for the continuation of business (a "Disaster Recovery Plan") to help ensure that Citi will continue to receive the services from alternate locations or with replacement Personnel no later than the applicable "Recovery Time Objectives" or "RTOs".

Suppliers are required to consult with the applicable primary Citi business contact to understand whether they are required to have a Disaster Recovery Plan and which of Citi's requirements are applicable to its Disaster Recovery Plan, including those with respect to RTO's which, if not otherwise defined in the applicable contract, are 4 hours or less for those processes rated by Citi as having a criticality rating of "1", 24 hours or less for those processes rated by Citi as having a criticality rating of "2" and 72 hours or less for those processes rated by Citi as having a criticality rating of "3".

Crisis Notification

Supplier will promptly notify the primary Citi business contact concerning any crisis, threat, warning or cyber event against Supplier or its sub-contractors that is reasonably likely to have an adverse impact on the services or products provided to Citi.

11.5 Testing

All of the Supplier's recovery resources and plans shall be tested annually at minimum and results of recovery tests shall be delivered to Citi within one week of the test date, in a format defined by Citi. Testing shall demonstrate the Supplier's ability to meet the recovery service levels for all products and services delivered to Citi.

Suppliers must provide Citi with at least 30 days' advance notice of testing the recovery of services provided to Citi. Citi may participate in, or observe Supplier's recovery testing.

Suppliers must test the following disruption scenarios:

a. Denial of Access (DOA)

1. Test that validates the staffing and support for Citi business processes that can be recovered within the defined RTO.

2. Prior to testing, Supplier must consult with Citi to reach agreement on the appropriate recovery strategy for its staff performing services for Citi, including the number of staff to be included in the testing exercise (which number shall, absent Citi's agreement otherwise, be at least 30% of the Personnel providing the services). Staff included in the testing exercise must work for a minimum of one business day from their alternate location.
3. Prior to testing, Supplier must consult with Citi to reach agreement on the evidence to be provided to Citi to show that Citi's recovery needs have been addressed, including the following:
    i. Evidence that work was processed at the remote, alternate, or transferred location for a minimum of one business day; and
    ii. A detailed description of any issues identified during the test including those that would render the test invalid.
4. All testing exercises must be designed to avoid any impact on production or any disruption or jeopardization of normal business operations
5. Supplier must promptly disclose to Citi any changes to its environment that would render invalid or would negatively affect the Disaster Recovery Plan.

b. Denial of Service (DOS)

1. Where Citi either logs in (signs on) to an application of or managed by Supplier or on Supplier's systems, Supplier must conduct, at least once annually in accordance with Citi requirements for each data center / technology room where these applications reside, a DOS test to demonstrate that the application can be recovered to the DR site specified in Supplier's Disaster Recovery Plan.
2. Both online and batch processing capabilities and both applications with and without user interfaces are in scope for DOS testing.
3. Prior to testing, Supplier will provide Citi with notice of and any information or assistance reasonably required to enable Citi to participate in the DOS testing. Supplier's notice of DOS testing will include:
    i. Supplier's Disaster Recovery Plan to the extent that Citi does not already have a current version;
    ii. The list of data centers / technology rooms and of the applications to be subject to the DOS test;
    iii. A description of any application dependencies that may limit Citi's ability to completely test the business process/functions in scope for the test; and
    iv. A description of any application components that will not be included in the DOS test.
4. Prior to testing, Supplier must consult with Citi to reach agreement on the evidence to be provided to Citi to show that Citi's recovery needs have been addressed, including the following:
    i. Evidence that the application(s) were recovered to the DR site specified in Supplier's Disaster Recovery Plan within the RTO specified in Supplier's Disaster Recovery Plan; and

ii. A detailed description of any issues identified during the test including those that would render the test invalid.

iii. All testing exercises must be designed to avoid any impact on production or any disruption or jeopardization of normal business operations.

iv. Supplier must promptly disclose to Citi any changes to its environment that would render invalid or would negatively affect the Disaster Recovery Plan

v. Scenario exercises that demonstrate the ability to recover in the event of a natural, man-made, technology or infrastructure event.

c. Citi Participation / Review of Supplier's Testing

For any test (including a retest) by Supplier of its Disaster Recovery Plan, Citi will engage in activity commensurate with Process Criticality / RTO:

1. Most Critical Applications / Processes to Citi Franchise. Citi will participate in or observe Supplier's testing activity for all processes and / or applications that it has defined as "Franchise Critical". For such processes and / or applications, Supplier permits Citi to review recovery plans covering business and / or technology (as applicable), test scripts, test results, and evidence.
2. Processes with an RTO < 24 hours. Unless otherwise requested by Citi, Citi need not participate/observe Supplier's testing activity, but will review recovery plans covering business and/or technology (as applicable) test scripts, test results, and evidence.
3. Processes with an RTO > 24 & < 72 hours. Unless otherwise requested by Citi, Citi will require Supplier's attestation for recovery planning covering business and / or technology (as applicable), test scripts, and test results.

d. Addressing Testing Findings

If any test results from Supplier's testing show a failure to meet any test objectives or any applicable RTO, Supplier will undertake to perform a source cause analysis and to remedy promptly any identified deficiencies. Following implementation of such remediation, Supplier shall conduct a retest not later than one hundred twenty (120) calendar days following the initial test failure (or the period of time specified in the relevant Work Order).

11.6 Crisis Management

In conjunction with its business continuity plan, the Supplier shall maintain a crisis management plan for command and control of recovery operations. At minimum, the Supplier's crisis management plan shall identify specific individuals of sufficient authority to activate a recovery operation, define communication and escalation protocols for gathering and disseminating crisis information and include notification and escalation protocols for communicating with Citi in the event of a crisis.

12 GLOBAL COMPLAINTS / CONCERNS MANAGEMENT STANDARDS

12.1 Overview

The Citi Complaints Policy establishes minimum requirements to develop Complaints / Concerns Management standards / procedures to address the identification, categorizing, handling and governance of Complaints / Concerns.

12.2 Identifying and Categorizing Levels of Complaints

Complaints / Concerns should be defined into three levels:

a. Level 1 Complaint / Concern:
   Is an expression of dissatisfaction at the initial consumer facing interaction
b. Level 2 Complaint / Concern:
   Is an expression of dissatisfaction escalated because it was unable to be resolved during the initial point of contact (Level 1) or the dissatisfaction is handled at Level 2 for business operational purposes
c. Level 3 Complaint / Concern:
   Is an expression of dissatisfaction received from regulatory channels, or addressed to senior executives from consumers directly alleging a violation of law or regulatory requirements, or contacts that could not be resolved during earlier interactions at Level 1 and / or 2.

12.3 Complaint Handling

a. Covered Business Transfer of Complaints / Concerns:

Suppliers must collaborate with Citi to develop procedures of when and how to refer or transfer complaints for handling to / from Citi.

b. Acknowledgement & Receipt of Complaints / Concerns:

In coordination with Citi, Suppliers must develop procedures to acknowledge the receipt of complaints consistent with regulatory requirements, customary practices, and desired customer experiences.

c. Investigation (Research) & Follow-Up:

1. In coordination with Citi, Suppliers must develop procedures that outline investigation and research requirements consistent with regulatory requirements, customary practices, and desired customer experiences. The Supplier is responsible for performing the necessary investigation and research in order to resolve the Complaints / Concerns with an informed conclusion.
2. In coordination with Citi, Suppliers must develop procedures that include follow-up requirements consistent with desired customer experiences. Additional information may be required in order to complete the Complaints / Concerns investigation and may require follow-up contact with the consumer.
3. In Coordination with Citi, Suppliers must have procedures in place to assess, analyze and escalate (concentrations of) complaints (in connection

with one employee or department) to ensure that potential internal fraud is detected.

d. Escalation

Suppliers must implement the following escalation processes:

1. Direct Escalation - Suppliers escalate the Complaints / Concerns directly to Level 3, with no de-escalation attempt permitted. The applicability should be further defined in the Regional Standards consistent with local laws, regulations, requirements, customary practices, desired customer experiences.
2. Consumer Requests - Suppliers are required to escalate the Complaints / Concerns, when a first attempt to de-escalate has failed and the customer requests to speak with a manager.
3. Entitlement/Policy Constraints - Suppliers are required to escalate the Complaints / Concerns, if the employee is not able to thoroughly research or provide appropriate resolution due to a lack of entitlement, authorization or operational policy constraints.
4. Consumer Demeanor (Supplier Discretion) - Supplier may offer to escalate if the consumer continues to express dissatisfaction. Supplier must consider if the consumer's reason for dissatisfaction suggests the resolution is not aligned with the local regulatory and Citi Fairness principals. The applicability must be further defined in the Regional Standards.

e. Response & Closure

Suppliers must comply with response and closure requirements:

- Include detailed explanation of the resolution
- Present in a style that is simple to understand
- Address each Complaint / Concern
- Include a description of actions taken
- Include how Citi can be reached if there are follow-up questions
- Include any supporting documents referenced in a written response
- Provide guidance that outlines appropriate communication methods within approved channels
- Outline situations when it may be appropriate not to respond to the Consumer
- Meet requirements for Legal and Compliance review and approval for response letters/templates

12.4 Resolution Standards – Service Level Standards for Response Resolution

Complaint / Concern Type Maximum Service Level Standard:

a. Level 1 - Closed within 1 business day, otherwise, escalate to Level 2

b. Level 2 - 90% Closed within 4 Business Days

c. Level 3 - 90% Closed within 30 Calendar Days, unless regulatory requirements direct a shorter timeframe or the Complaint / Concern is with an External Legal Attorney or Court

12.5 Capture – Required Data Elements

Consistent application and implementation of Complaints / Concerns data elements provide measurable reporting and facilitate in identifying potential key risk indicators for effective Complaints / Concerns analysis. Suppliers must capture the following information for each complaint: Receipt Date, Complaints / Concerns Date, Line of Business, Employee ID, Account / Application Number, Product or Service Name / Description, Source of Contact / Channel Received, Complaint / Concern Categorization, Disposition – Controllable (Bank Error) Level 3 Only, Fairness Related and Closed Date.

In addition to the fields above, Suppliers must document the following for each complaint:

a. Complaints / Concerns Description – As described by the Consumer

b. Complaints / Concerns Research – Actions taken to research and resolve

c. Complaints / Concerns Closure – Response information provided to the Consumer

Suppliers must provide Citi complaint data on a periodic basis as agreed upon by the Supplier and Citi.

12.6 Call Recording and Call Retention

Suppliers must implement a process for recording and storage of all calls related to Complaints / Concerns for at least 12 months from the date of the call unless otherwise directed by local regulatory requirements.

13 GLOBAL BACKGROUND SCREENING STANDARDS

13.1 Overview

The purpose of this Section is to define Citi's global standards for background screening for Suppliers. Background screening must be performed in accordance with all applicable local laws and regulations for all Suppliers' Personnel that will have access to Citi proprietary or Confidential Information, systems and / or unescorted access to Citi facilities.

Additional information on country-specific requirements and exceptions to these standards can be found here.

All information and self-disclosures described within this document must be provided by Supplier's Personnel as appropriate. Falsification or omission of information whether on a resume, during the interview, on an on-boarding form or during the on-boarding process, no matter when discovered, may constitute grounds for denial or termination of assignment with Citi in accordance with local law. Adverse results to any screening performed, no matter when discovered, may also constitute grounds for denial or termination of assignment with Citi in accordance with local law.

Citi may, at any time, request information validating that any individual a Supplier intends to assign or has assigned to perform services for Citi, has successfully completed all background screening requirements according to these standards and applicable local law and regulations.

13.2 Collection of Basic Information and Identity Verification

Prior to any Supplier's Personnel beginning a Citi assignment, Suppliers must collect the individuals' first and last name, mailing address and permanent address (if different), telephone number and e-mail address (if applicable).

Supplier's Personnel must also provide documentation which validates their identity. This may include providing information and / or documentation of a national ID number, a government-issued identification card with a picture or a passport.

13.3 Sanctions Screening

All Supplier Personnel must be screened, against the United States Department of the Treasury's Office of Foreign Assets Control ("OFAC"), Specially Designated Nationals and Blocked Persons ("SDN") list and the list of regions and jurisdictions subject to sanctions imposed by the United States ("U.S. Sanctions"), as well as any other non-US sanctions lists appropriate to the legal jurisdiction in which the assignment is located. This includes using names, addresses, aliases and date of birth provided from the verification process, prior to their first day of assignment (except where not allowable by local law). Supplier Personnel who are positively matched to a sanctions list entry are prohibited from working on the Citi assignment. Any indication or misrepresentation may result in the ineligibility for or closure of, the assignment.

When key Personnel Information described above is changed for any assigned individual, all information for that individual must be rescreened against the aforementioned sanctions lists.

Any Supplier Personnel who are positively matched to a sanctions list entry upon rescreening are to be removed from the Citi assignment immediately.

13.4 Immigration Compliance

Supplier must demonstrate that it has protocols for verifying that its Personnel are authorized to work in the countries where they are assigned, and that Supplier has complied with all applicable laws and regulations to verify employment eligibility. Supplier further must demonstrate that it has protocols for ensuring that its Personnel are otherwise in compliance with all applicable immigration laws and regulations and that its Personnel hold the appropriate classification of visa for the assignments and activities in which they are engaged.

13.5 Employment History

Suppliers are to validate the employment history of its Personnel for the past seven (7) years. The individual's employment history must be validated to ensure that the employers, positions, dates and duties have been accurately represented.

Supplier's Personnel must also disclose any prior employment or assignment as a consultant or temporary worker with Citi or any of its predecessor companies (including, but not limited to: Citibank, Citicorp, Travelers, Salomon Brothers and / or Smith Barney). They must also disclose whether they have been terminated by, asked to resign by or denied employment or assignment after receiving an offer from, Citi or any of its predecessor companies.

13.6 Education History

Suppliers are to validate the highest level of education of its Personnel. The information validated should include the dates attended, institution name(s), address(es) and degree(s) obtained.

The highest level of education that the individual has provided must be validated to ensure that the dates attended, institution, and qualification obtained have been accurately represented. This may be done by contacting the institution directly or by reviewing / authenticating letters, transcripts and diplomas issued by the institution, as appropriate.

13.7 Criminal Background

Where legally permissible, Suppliers' Personnel are to disclose any criminal convictions, guilty plea or no contest plea (including any pre-trial diversion program) before any court for any criminal offense.

The administrative review of criminal records and / or fingerprint checks is to be initiated prior to the assignment start date where legally permissible and available.

Criminal convictions for offenses relating to theft, fraud, dishonesty or breaches of trust, except where otherwise prohibited by law, may result in denial of and / or ineligibility for, assignment with Citi. Other convictions may result in denial of and / or ineligibility for assignment based on applicable local laws and regulations. Assignment decisions contingent on criminal convictions must be in accordance with local laws and regulations.

13.8 Drug Screening

Where legally permissible, Suppliers are to ensure that its Personnel complete a drug screening test prior to commencing the assignment with Citi. At a minimum, the drug screen must be a "5-panel" test, which tests for the presence of amphetamines, cannabinoids (THC), cocaine, opiates and phencyclidine (PCP). Positive results are to be adjudicated by a medical practitioner and are sufficient to deny assignment, whether results are received prior to or after the commencement of work, except for where not allowable by local law.

Certain Supplier Personnel may be asked to complete a drug screening test during their assignment because of the requirements of the position (e.g., drivers, pilots) or for other reasons in accordance with local laws and regulations.

13.9 Credit Check

Suppliers may perform a credit check for its Personnel assigned to Citi in designated positions or positions which involve advising Citi Clients on financial products and / or investments or where it is a local practice and legally permitted. Assignment decisions based on credit checks must be in accordance with local laws and regulations.

13.10 Re-screening

Supplier's Personnel whose assignment terminates must be re-screened in the event they are reassigned to Citi. For additional information on re-screening requirements, please refer to "Table 2: Re-screening by Length of Break in Service" below.

13.11 International Transfers

All screening must be completed in accordance with the regulations of the country where the assignment is located. If Supplier's Personnel transfer to a new country and there is a break in service with Citi, the individual must be re-screened according to the requirements of the new country. For additional information on re-screening requirements, please refer to "Table 2: Re-screening by Length of Break in Service" below.

Table 1: Background Screening Completion Timing

Type	Required	Self-Disclosure	Verification	Initiation	Completion	Description
Sanctions Screening	X		X	Before start	Before start	Supplier's Personnel must be checked against appropriate local government or agency control lists using names, aliases, addresses, and date of birth provided.
Identity Verification	X	X	X	Before start	Before start	National ID number and documentation is provided which validates identity.
Immigration Compliance	X	X	X	Before start	Before commencement of services to Citi	Evidence of visa compliance and employment eligibility verification as required by applicable laws and regulations.
Employment History Verification	X	X	X	On or before start	≤90 days after start	Verification of past seven (7) years of employment.
Education History Verification	X	X	X	Before start	≤90 days after start	Verification of the dates, institution and degree of the highest level of education.
Criminal Background Check	X	X	X	Before start	Before start	Check of any conviction, guilty plea or no contest plea in any court, an administrative review of available records and / or fingerprint check (where legally permissible and available).
Drug Screening	X		X	On or before start	≤5 days after start	"5-panel" test for presence of amphetamines, cannabinoids (THC), cocaine, opiates and phencyclidine (PCP) (in accordance with local laws).
Credit Check			X	On or before start	≤90 days after start	May be performed where legally permitted for workers in positions which involve advising Citi Clients on financial products and / or investments. May also be performed where it is a local practice.

Table 2: Re-screening by Length of Break in Service

Type	Any Break	7 days < Break ≤ 30 days	Break > 30 days
Criminal Background Check	X	X	X
Drug Screening		X	X
Sanctions Screening		X	X
Full screening[1]			X

[1]Background screening components that 1) would not return any new or different results and 2) are not required by law, or for other reasons, upon the commencement of assignment, do not require re-screening (e.g., Education Verification), as long as it can be confirmed that the screening was performed in the past and that records related to the screening were retained.

APPENDIX A - DEFINITIONS

Affiliate is any entity that directly or indirectly controls, is controlled by or is under common control with Citi, where "control" means the ownership of or the power to vote, at least twenty percent (20%) of the voting stock, shares or interests of such entity.

Background Screening is the process of verifying information provided by Supplier's Personnel and compiling relevant records (i.e., criminal, drug, etc.) about their background.

Business Activity Owner (BAO) is a Citi employees responsible for performing and actively managing certain activities associated with Supplier relationships.

Business Gift is any item of value (other than Business Entertainment) given or received by a Citi employee in connection with Citi's business or the business of the external party, generally excluding items valued at USD $25 or less.

Citi Approved Supplier Program (CASP) is Citi's global program that promotes standard Supplier risk management processes and control assessments across the enterprise to mitigate Citi's compliance, transaction, financial, strategic, technology and reputation risk with Suppliers, while encouraging Supplier consolidation to maximize Citi's economic leverage. The CASP system hosts Citi's corporate-wide Approved Supplier list, enables Citi Businesses to more effectively manage Approved Suppliers and provides a central location for Businesses to: identify and classify Suppliers based on various characteristics and risk attributes such as business criticality, OSP designation, access to Confidential or higher Information and spend thresholds; view Supplier and Citi points of contact; review Supplier due diligence information; and access Supplier risk management reports and scorecards.

Citi Information refers to any type of Information that is owned by Citi and which Citi is obligated to protect.

Client shall mean any client or customer of Citi and may include individuals (i.e., natural persons) as well as businesses, institutions, organizations and legal entities.

Computer means an electronic, magnetic, optical, electrochemical, or other data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

Computer program means data representing instructions or statements that, when executed in a computer, causes the computer to perform a function.

Computer system means an arrangement of interconnected computers that is designed to perform one or more specific functions, and includes: (a) an information technology system; and (b) an operational technology system such as an industrial control system, a programmable logic controller, a supervisory control and data acquisition system, or a distributed control system.

Confidential Information is information that Citi Businesses are obligated to protect including, but not limited to, information belonging to: Clients, customers, employees, third parties or Citi Businesses.

Confidential Personally Identifiable Information (PII): PII will have an information protection classification of Confidential if the compromise of confidentiality, integrity or availability of PII could reasonably be expected to have a serious adverse effect on the affected individuals or Citi, the compromise of confidentiality, integrity or availability of the PII would trigger breach notification requirements under applicable law. A serious adverse effect to an individual means that the impact could reasonably result in moderate financial loss or fraud, or personal embarrassment or distress.

Examples of data elements when combined with other information constitutes Confidential PII:

a. Individual name or contact information (address, telephone, or email address) in combination with:
    1. Passport number, driver's license number, national or government ID number, or an individual's tax ID number;
    2. Customer Identification number, Credit / Debit card number, Account identifiers that may result in funds movements, or other financial account number;
    3. Transactional data elements that can be used for identity theft or fraud;
    4. Customer account application information, credit report data, credit score;
    5. Worker performance appraisal or compensation information;
    6. Video recordings including CCTV and ATM records.

These elements are considered Confidential PII either alone or in combination with other elements.

b. A U.S. Social Security number or government issued identification number (that is equivalent in usage and / or legal protection status to the U.S. Social Security number) alone or any financial account number alone that can be used for ID theft or fraud.

Contract is a written legal document signed by two or more parties that includes an offer, acceptance, consideration, obligations of the parties and legality of purpose. Examples of Contracts may include Master Agreements for products and services, statements of work / work orders, amendments and addenda, schedules, orders or any other written document signed by a Citi entity and a Supplier. A Non-Disclosure Agreement (NDA) is also considered a Contract for the purposes of these Standards.

Core Business Process Outsourcing (Core BPO) is a function, operation or service that if unable to be provided, would impact a Citi Business' ability to operate effectively, to deliver its products and services and / or to comply with applicable legal and regulatory requirements. Core BPO may include, but is not limited to, loan processing; deposit processing; fiduciary and trading activities; Internet banking services; treasury operations; merchant processing services; records management services and customer call centers (inbound or customer care / service). For the purpose of this policy, internal audit and compliance functions are also considered Core BPO.

Critical Data Assets (CDA) are those electronic repositories (datasets or databases supporting business applications) that contain, customer information, employee or other information that represents a financial or reputational risk to Citi and/or may introduce fraud, identify theft or financial risk to our customers or businesses.

Enterprise Supply Chain (ESC) is Citi's global organization with responsibility for support of the end-to-end Supplier lifecycle process, from Supplier risk assessment, to competitive bidding and selection, contracting and payment. Specific activities include appropriate Supplier due diligence to ensure continued delivery of critical goods and services to our business partners, Supplier on-boarding, strategic sourcing, Contract negotiations for a wide variety of products and services, buying and order fulfillment, payment processing, as well as diverse and sustainable Supplier initiatives.

Functional IDs are a generic ID, such as ADMIN or ROOT, that is used by a person or process to access a security system. A key initiative in the Identity and Access Management (IAM) operation is ensuring that Citi has specific, defined controls in place to protect against the risks surrounding the use of Functional IDs.

Information Classification

Restricted is Information that, if disclosed to any unauthorized person, including people who work at Citi, could have significant impact on Citi's legal and regulatory obligations or on its financial status, customers or Franchise.

Confidential is Information that Citi Businesses are obligated to protect including, but not limited to, information belonging to customers, workers, third parties or Citi Businesses. Confidential information is any combination of data subject to regulatory or contractual restrictions on disclosure. It is also information that the businesses determine that if disclosed to unauthorized individuals, has the potential to provide a competitive advantage or have a significant negative impact on the business.

Confidential PCI is an all credit, debit or prepaid card account information for cards branded by Card Association members (Visa, MasterCard, American Express, Discover and JCB) that is stored, processed or transmitted and would facilitate credit or other financial fraud against an individual:

For example, PAN (Primary Account Number) by itself, or any combination of data elements including but not limited to: Cardholder Name, Service Code, Expiration date, CVV.

Internal information is commonly shared within Citi, is not intended for distribution to anyone outside of Citi and is information that is not classified as Restricted or Confidential. Examples of Internal information include our policies and standards.

Public is information that is freely available outside of Citi or is intended for public use, like Citi press releases or articles that appear in the news about Citi.

Confidential or Higher is defined as Confidential, Confidential PII, Restricted or Authentication*.

***Authentication** is a separate classification with its own requirements as defined within these Standards. It is completely independent of other Information Classifications.

Internal PII will have an information protection classification of Internal if the compromise of confidentiality, integrity, or availability of PII could be expected to have a limited adverse effect on the affected individuals. A limited adverse effect means that the impact to the affected individuals has a low potential for financial loss, and does not involve the

compromise of sensitive personal data or impact the human rights of the individual, and would not expose Citi to greater than minor financial or reputational loss.

Examples of Internal PII (in any combination) can include:

- IP addresses or media access control address (MAC)
- Cookie ID's
- Contact Information = Citi employee name, work email address
- Business Contact Data = Work address, phone, email, general business card information
- Employee SOEID or GEID

Information security or "IS" means the state in which a computer or computer system is protected from unauthorized access or attack, and because of that state, (a) the computer or computer system continues to be available and operational; (b) the integrity of the computer or computer system is maintained; and (c) the integrity and confidentiality of information stored in, processed by or transmitted through the computer or computer system is maintained.

Information Technology Outsourcing (ITO) is Outsourcing to a Supplier all or a significant part of a Citi Business' information technology (IT) function, operation, role or service that may include, but is not limited to, system development and maintenance, production support, security monitoring and testing, network operations, web hosting services and help desk operations supporting systems.

IS Threat means act or activity (whether known or suspected) carried out on or through a computer or computer system, that may jeopardize or affect adversely, the IS of that or another computer or computer system.

IS Vulnerability means any vulnerability in a computer or computer system that can be exploited by one or more IS Threats.

Master Agreement is a Contract negotiated by a Citi entity that establishes consistent terms and conditions and allows, but typically does not obligate, Citi entities to procure products and services from the Supplier pursuant to the Master Agreement by executing transactional documents in the form of schedules and orders. The Master Agreement may reflect a negotiated pricing schedule or pricing may need to be separately negotiated as part of the negotiation of the applicable transactional document.

Non-Core Business Process is a function, operation or service that is not a Core BPO. Non-Core Business Processes may include, but are not limited to, mailroom operations, property management and relocation services.

Non-Disclosure Agreement (NDA) is an agreement between Citi and a Supplier whereby the exchange, use and disclosure of Information is governed by the terms of the agreement.

Outsource Service Provider (OSP) is an external or Affiliate service provider that has an arrangement with a Citi Business to operate, perform or manage all or a significant part of a business function, role, service or system operation that was at one time performed internally by the Citi Business or would ordinarily be performed internally by a similar business. In these arrangements, Citi maintains the responsibilities of setting standards, measuring actual performance and taking appropriate corrective action, when applicable. OSPs do not include services where the Citi Business retains direct management control

of the service received, such as third party maintenance Contracts; legal, audit or other professional services; consultants or temporary staff working under Citi direction. Direct Management control may include managerial functions such as planning, organizing, staffing and directing. A relationship with an OSP may involve a Core Business Process Outsourcing, Information Technology Outsourcing or a Non-Core Business Process:

Outsourcing is an arrangement for an external or Affiliate service provider to operate, perform or manage all or a significant part of a Citi business function, role, service or system operation that was at one time performed internally by the Business or would ordinarily be performed internally by a similar business. This does not include services where Citi retains direct management control of the service received, such as third party maintenance Contracts; legal, audit or other professional services; or consultants or temporary staff working under Citi direction. Outsourcing may include three types of business agreements:

(1) Agreements between a business unit and an Outsource Service Provider (OSP) located in the same country (i.e., Domestic Outsourcing / Onshore Outsourcing).

(2) Agreements between a business unit and an OSP located in different countries, including arrangements with Suppliers within close geographical proximity to the Business (i.e., Nearshore Outsourcing) and arrangements with Suppliers in a different geographical region than the Business (i.e., Offshore Outsourcing). For the purpose of this policy, “Offshore” refers to both “Offshore” and “Nearshore” Outsourcing arrangements.

(3) Intra-Citi Service Agreements (ICSAs) are legal agreements between two or more Citi Affiliates. In certain situations, under applicable laws in certain jurisdictions, ICSAs must reflect an arm’s length transaction and payment terms based on market rates. ICSAs may also be known as “Inter-Affiliate Agreements.” ICSAs may be Domestic or Offshore Outsourcing

Personally Identifiable Information (PII) is any information that relates to and identifies or can be used to identify a living individual. PII may relate to any living individual, including current and past Citi Clients, customers, applicants for Citi products or services, personnel or Citi Suppliers, Citi staff and their dependents, applicants for Citi jobs and any other individuals.

Personnel as used in this policy refers to a Supplier’s officers, employees, agents, auditors, consultants, contractors and sub-contractors, as well as the directors, officers, employees, agents, auditors, consultants or other representatives of any affiliate, contractor or sub-contractor utilized by Supplier to provide any products or services to Citi.

Privilege: A basic principle in information security that holds that entities (people, processes, devices) should be assigned the fewest privileges consistent with their assigned duties and functions. For example, the restrictive "need-to-know" approach defines zero access by default and then opens security as required. All data in a corporate network would be off-limits except to specific people or groups

Public PII: Personally Identifiable Information that is available publicly and lawfully outside of Citi and is intended for public distribution.

Restricted PII: Restricted PII will have an information protection classification of Restricted if the compromise of confidentiality, integrity or availability of PII could reasonably be expected to have a severe or catastrophic adverse effect on affected individuals or Citi or if, under the law of the jurisdiction, increased security controls are required due to the nature of the PII, (e.g., sensitive or 'special category' PII).

A severe or catastrophic adverse effect to an individual means that the impact could reasonably result in significant adverse effects to the individual, including the financial loss, loss of employment or loss or difficulty in obtaining employment, loss of human rights, personal or public humiliation or inappropriate imprisonment.

Examples of Restricted PII include any information from Public PII, Internal PII and Confidential PII in combination with:

Data specifically relating to: race, religion, religious or philosophical beliefs, ethnicity, political affiliation or opinions, union membership, criminal background information or criminal offenses, genetic data, biometric data, or data regarding an individual's sexual orientation or activity.

Personal Health information (PHI) which includes information regarding the individual's medical history or mental or physical condition; the provision of health care to an individual and the payment for the provision of health care to the individual.

Records Information that Citi is obligated to retain for legal, regulatory or approved business reasons.

Records Inventory is a detailed listing that includes the record types, location, dates, etc., of Citi's records and is needed for a business to properly manage their records through the Information Lifecycle.

Record Hold is a requirement placed on Records and Information that suspends modification or disposal until lifted by the authority that issued the hold.

Restricted Information is information that, if disclosed to unauthorized individuals, could have a significant impact on Citi's legal or regulatory obligations or on its financial status, customers or franchise.

Sanctions Screening includes the OFAC SDN List, the list of regions and jurisdictions subject to sanctions imposed by the United States ("U.S. Sanctions") as well as any other U.S. Sanctions programs, as well as any list issued and jurisdictions subject to sanctions not imposed by the United States, pursuant to local sanctions laws and regulations ("Non-U.S. Sanctions") applicable as well as any other non-U.S. Sanctions programs.

Sensitive Data is data classified as Authentication, Restricted, Restricted PII, Confidential, Confidential PII, Confidential PCI or where use of the data is restricted by local laws and regulations.

ESC Sourcing Manager is an individual within Enterprise Supply Chain who is responsible for the negotiation of Contract business terms, requirements and pricing, including RFP's and other Supplier selection activities, administration to the Contract terms and conditions and financial evaluation accreditation requirements. The ESC Sourcing Manager is also responsible for engaging legal support, if required, to assist with the negotiation of the legal terms and conditions.

Supplier is any third party, together with its employees, agents or representatives, that provide products and / or services to Citigroup Inc. or any of its Affiliates, including its subsidiaries (collectively or individually, such entities being referred to herein as “Citi” or the “Company”).

Third Party is an individual or entity that has entered, or may enter, into a business arrangement, by Contract or otherwise, to provide products or services to a Citi Entity or otherwise has an ongoing business relationship (other than a customer / consumer or employee relationships) with Citi.

Third Party Officers (TPOs) report into the Businesses / Global Functions and are responsible for performing certain activities within the Third Party Relationship Life-Cycle. TPOs are responsible primarily for monitoring Tier 1, 2 and 3 Third Party Relationships and work with the Business, Operations and Technology (O&T) teams, as well as other Citi functions, to maximize the Businesses’ engagement with the Third Party and also to identify, manage and mitigate risk throughout the Third Party Relationship Life-Cycle.

Utility Program is a program, tool, product, or application that does not typically execute business logic but is used to facilitate the operation of specific tasks related to the management of computer functions.