# Table of Contents

1. General Overview  .......................................................... 3
2. Equal Employment Opportunity / Affirmative Action .................. 4
3. Anti-Bribery and Corruption (AB&C) .................................. 6
4. Gift and Entertainment ...................................................... 6
5. Supplier Diversity & Supplier Principles .................................. 7
6. Prohibition Against Modern Slavery ..................................... 7
7. Supplier Personnel ........................................................... 9
8. Fraud Management ........................................................... 10
9. Media Interaction and Public Appearances ............................. 12
10. Written Electronic Communications ...................................... 12
11. Political Activities and Contributions .................................. 13
12. Anti-Money Laundering ("AML") ......................................... 13
13. Records Management ....................................................... 14
14. Customer-Facing Services .................................................... 15
15. Enterprise Resilience / Continuity of Business ....................... 19
16. Global Background Screening Standards ............................... 25
17. Expenses ............................................................................. 27
18. Information Security (IS) .................................................... 28
19. Secure Workplace Guidelines ............................................. 55
20. Artificial Intelligence/Machine Learning ................................. 56

Appendix - Definitions ............................................................ 58
1 GENERAL OVERVIEW

1.1. Requirements Generally

These Citi Requirements for Suppliers ("Requirements") detail some of the obligations that Suppliers must meet in the course of doing business with Citi. Certain Requirements are applicable to all Suppliers, while the applicability of other Requirements to a particular Supplier depends upon the types of product(s) and service(s) that Supplier provides to Citi (the latter are summarized in Section 1.2 below and is indicated at the beginning of each provision listed therein). Capitalized terms shall have the meanings ascribed to them herein, including in the attached Appendix, unless no such meaning is herein indicated, in which event it shall have the meaning ascribed to it in the Contract, as defined below.

These Requirements are contractual obligations under Supplier agreements with Citi (including, but not limited to, transactional documents, e.g., work orders, license schedules) (each a "Contract"), and are in addition to any obligations specified in any Agreement, any obligations under Applicable Law (as that term is defined below), any notice to Supplier from Citi informing Supplier of its obligations under the same (each a "Notice"), or any additional more specific requirements implemented by Citi’s businesses or functions. The more restrictive obligations and requirements shall apply to the extent of any conflict between any of the foregoing requirements and the Restrictions. Suppliers must take a proactive role and consult with their primary Citi business contact (or designee) regarding any questions they have regarding these Requirements, including any changes thereto, any requested exemption therefrom, or any perceived conflict therein or with Applicable Law.

Supplier shall promptly comply with any reasonable request that Citi may submit to Supplier for data that Citi requires related to Supplier Services or Personnel in association with Citi’s obligation to comply with Applicable Laws. Supplier’s failure to comply with these obligations shall be deemed a material breach of the terms of this Agreement.

Failure to comply with these Requirements, or any additional requirements specified by a Citi business with which Supplier does business may result in termination of a Supplier’s Contract with Citi. Furthermore, violations of the Requirements 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. Suppliers may not use compliance with its own policies as a substitute for its obligation to comply with any provisions of these Requirements without Citi’s written consent.

1.2. Requirements Applicable to Selective Suppliers

The following chart lists certain Requirements which apply to certain Suppliers who meet the applicability criteria designated therein. Sections not mentioned below are applicable to ALL Suppliers.

<table>
<thead>
<tr>
<th>Section #</th>
<th>Section Title</th>
<th>Applicability</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>ANTI-MONEY LAUNDERING</td>
<td>Applicable to Suppliers performing certain customer-related services (i.e., on-boarding, customer account and transaction)</td>
</tr>
<tr>
<td>Section #</td>
<td>Section Title</td>
<td>Applicability</td>
</tr>
<tr>
<td>-----------</td>
<td>---------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>13</td>
<td>RECORDS MANAGEMENT</td>
<td>Applicable to Suppliers who access/process/store Citi Information</td>
</tr>
<tr>
<td>14</td>
<td>CUSTOMER – FACING SERVICES</td>
<td>Applicable to Supplier interacts with any individual in such individual’s capacity as a past, current, or potential customer of Citi or of a related party (such as an employee or a representative) of such customer (each such individual, a “Customer”).</td>
</tr>
<tr>
<td>15</td>
<td>CONTINUITY OF BUSINESS</td>
<td>Applicable to Suppliers who are included in the Recovery Plan for the Citi Business unit or if the supplier hosts an application with recovery capabilities (i.e., numeric Technology Recovery Time Capability (TRTC)), which is used by Citi. The Citi Business Activity Owner (BAO) is responsible for communicating applicability and COB requirements to the Supplier.</td>
</tr>
<tr>
<td>16</td>
<td>GLOBAL BACKGROUND SCREENING STANDARDS</td>
<td>Applicable to Suppliers whose personnel has access to Citi systems/networks; AND/OR unescorted access to Citi premises; AND/OR utilize Subcontractors (Such personnel would be required to have a GEID, and be registered in Citi’s Non-Employee Management System); AND/OR Suppliers that access/process/store/manage Citi Confidential or Higher Information</td>
</tr>
<tr>
<td>17</td>
<td>EXPENSES</td>
<td>Applicable to Suppliers that are contractually eligible to claim reimbursable business expenses</td>
</tr>
<tr>
<td>18</td>
<td>INFORMATION SECURITY (IS)</td>
<td>Applicable to Suppliers including Subcontractors that access/process/manage/store Citi Information; AND/OR Suppliers responsible as a Host for Citi branded internet facing applications; AND/OR Suppliers with connectivity to Citi’s network resources; AND/OR Suppliers requiring unescorted access to Citi facilities.</td>
</tr>
<tr>
<td>19</td>
<td>SECURE WORKPLACE GUIDELINES</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>ARTIFICIAL INTELLIGENCE/MACHINE LEARNING</td>
<td>Applicable to Suppliers that utilize Artificial Intelligence/ Machine Learning (AI/ML), as defined by Citi in any part of the product/service that they are providing.</td>
</tr>
</tbody>
</table>

2 **EQUAL EMPLOYMENT OPPORTUNITY / AFFIRMATIVE ACTION**

As part of our efforts to comply with federal non-discrimination and affirmative action regulatory requirements, Citi has developed an Equal Employment Opportunity and
Affirmative Action program and policies which are designed to ensure equal employment opportunities to all qualified persons without regard to race, color, religion, sex, sexual orientation, gender identity, national origin, citizenship, immigration status, age, marital status, genetic information, disability, protected veteran status or any other reason prohibited by law.

This includes, but is not limited to, the following:

a) Hiring, placement, transfer, demotion, or promotion
b) Recruitment, advertising, or solicitation for employment
c) Treatment during employment
d) Rates of pay or other forms of compensation
e) Selection for training, including apprenticeship
f) Layoff or termination

Suppliers shall comply, and shall cause its Personnel to comply, with the requirements of all applicable non-discrimination and affirmative action laws and regulations, including, but not limited to, any such laws or regulations that Citi notifies Supplier in writing that it must comply with.

Refer to Citi’s U.S. Equal Employment Opportunity and Affirmative Action Policy Statement for more information, which may be found at U.S. Equal Employment Opportunity and Affirmative Action Policy Statement (citibank.com)

2.1 Digital Accessibility Expectations for Existing Suppliers or Partners

Digital Accessibility Compliance – All digital properties and platforms interfacing with Citi employees or customers and produced by an existing vendor or subcontractor must comply with digital accessibility requirements and all applicable laws relating to accessibility. Supplier must ensure compliance with Web Content Accessibility Guidelines that provide equal or greater accessibility than WCAG 2.0 AA, such as WCAG 2.1 AA, developed by the Accessibility Guidelines Working Group of the World Wide Web Consortium (W3C) Web Accessibility. Evidence of compliance with the Web Content Accessibility Guidelines must be provided to Citi on an annual basis and prior to renewal of the Agreement. Any WCAG deficiencies found in accessibility testing shall be resolved within the timelines provided by Citi to Supplier that correspond to the severity of the defect.

2.2 Digital Accessibility Expectations for New Suppliers or Partners, including New Partner-Hosted Credit Processes

Digital Accessibility Compliance – All digital properties and platforms interfacing with Citi employees or customers and produced by a new vendor or subcontractor must comply with digital accessibility requirements and all applicable laws relating to accessibility. Supplier must ensure compliance with Web Content Accessibility Guidelines that provide equal or greater accessibility than WCAG 2.0 AA, such as WCAG 2.1 AA, developed by the Accessibility Guidelines Working Group of the World Wide Web Consortium (W3C)
Web Accessibility. Evidence of compliance with the Web Content Accessibility Guidelines must be provided to Citi on an annual basis and prior to renewal of the Agreement. Any WCAG deficiencies found in accessibility testing shall be resolved within the timelines provided by Citi to Supplier that correspond to the severity of the defect.

3 ANTI-BRIBERY AND CORRUPTION (AB&C)

Citi has policies, procedures, and internal controls reasonably designed to comply with AB&C laws, and strictly prohibits bribery or facilitation payments in any form. Suppliers, their Personnel, or anyone acting on Citi’s behalf, directly or indirectly, shall conduct their activities in accordance with the highest ethics standards and in compliance with all applicable AB&C laws and regulations, including the U.S. Foreign Corrupt Practices Act (FCPA), the U.K. Bribery Act (UKBA), each, as amended, and the applicable local AB&C laws of the countries in which Citi operates.

Neither Supplier, nor any of its Personnel, operating on Citi’s behalf, (i) will make, confer, authorize, or offer any payments, benefits, advantages, or other things of value to person; or (ii) receive or accept any payment, benefit, or other advantage from any person, in each of case (i)-(ii) in violation of AB&C laws. Supplier and its Personnel must conduct their activities and transactions on behalf of Citi in compliance with the applicable Requirements in this Standard, including this Section. Supplier and its Personnel must also maintain an AB&C compliance program, and policies and procedures designed and applied to ensure its compliance with all AB&C laws.

For an overview of Citi’s AB&C Program, please visit Citigroup’s Investor Relations (under Citi Policies, select AB&C Program).

4) GIFT AND ENTERTAINMENT

Neither Suppliers, nor their Personnel, may 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 including gift cards, gift certificates, red envelopes and vouchers are not permitted under any circumstances and Suppliers and their Personnel must not provide non-cash Business Gifts exceeding, in aggregate, U.S. $100 per person per calendar year to a Citi employee. Any Citi 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 businesses, 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. If Supplier is not in attendance at the event, the entertainment will be considered as a Business Gift. 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.

5) SUPPLIER DIVERSITY & SUPPLIER PRINCIPLES

Citi has implemented a Supplier Diversity Program which, among other initiatives, encourages the use of businesses certified as being owned by minorities, women, disabled individuals or veterans as suppliers and Subcontractors (“Diverse Suppliers”) to the fullest extent possible to assist Diverse Suppliers in their growth and development on a long-term basis. To assist Citi in complying with these goals, Supplier will, consistent with its other obligations hereunder and to the extent it is using Subcontractors or otherwise purchasing goods or services in connection with Supplier’s performance of its obligations under this Contract, make good faith efforts to allocate not less than fifteen percent (15%) of the amount Supplier is spending with respect to its Subcontractors towards goods and services sourced from Diverse Suppliers. Supplier will provide Citi with information relating to Supplier’s expenditures, either direct or indirect, with Diverse Suppliers by completing a “Diversity Profile Tier 2 Form” (which Citi may provide on a quarterly basis) and sending the completed form to Citi within fourteen (14) calendar days following the later of:

a) the close of the quarter during which Citi submits a Diversity Profile Tier 2 Form to Supplier, or

b) the date Supplier receives a Diversity Profile Tier 2 Form from Citi.

Citi will keep and treat all Diversity Profile Tier 2 Forms in accordance with Citi’s confidentiality obligations as set forth in Appendix E. Supplier will submit all completed Diversity Profile Tier 2 Forms to the attention of the Citigroup Supplier Diversity Program, 388 Greenwich Street, 19th Floor, New York, NY 10013, attention Director, Supplier Diversity Program. Additional information is available on the site Doing Business with Citi, which describes Citi’s additional expectations for Suppliers that may be found in:

Citi Statement of Supplier Principles
Citi Sustainable Progress Strategy
Environmental and Social Policy Framework
Citi Statement of Human Rights

6 PROHIBITION AGAINST MODERN SLAVERY

Citi is committed to implementing systems and controls aimed at identifying and addressing the risk that modern slavery and human trafficking could take place within its organization or in any of its supply chains. All of Citi’s Suppliers shall adhere to the Requirements set out below, and to develop effective enterprise-wide policies and procedures to identify and address the risk of modern slavery and human trafficking within their own operations and supply chains. Suppliers are required to complete Citi’s
Corporate Responsibility Questionnaire at Citi’s request to enable Citi to assess risk exposure and potential mitigation steps, particularly for Suppliers in higher-risk sectors and geographies.

6.1 Child Labor Avoidance. Supplier shall not employ child labor. 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 youngest. 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.

6.2 Freely Chosen Employment. Supplier shall ensure that workers are not forced, mentally or physically coerced, bonded, indentured, or subjected to involuntary prison labor or slave trafficked or subjected to compulsory labor in any form, including forced overtime. All work must be carried out voluntarily. Supplier’s obligations hereunder include, but are not limited to, ensuring the following:

1. **Contracts, Wages and Working Hours:** 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 honored by the employer and shall meet industry standards and the minimum requirements of applicable laws and collective agreements where the work is carried out.

2. **Right to Freely Terminate Work:** 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.

3. **Inhumane Treatment:** 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.

4. **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.

5. **No Confiscation of Identity Documents:** 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.

6. **No Recruitment Fees or Debt Bondage:** 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. 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.

7. **Freedom of Movement:** 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.

8. **Grievances without retaliation:** 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 victimization for having raised a grievance.

## 7 SUPPLIER PERSONNEL

### 7.1 Supplier’s Personnel Training, Assignment, Re-Assignment and Management

Supplier will use adequate numbers of individuals with suitable training, education, experience, and skill to perform the Services in the most effective manner consistent with any Contract and will substantiate the qualifications of such individuals upon request. After Personnel have been assigned to a Project, Supplier will not reassign or utilize any Personnel for other matters that reduces his/her availability to work on the Project without the prior written consent of Citi and will generally assign Personnel on Projects a manner that minimizes disruptions caused by the need for reorientation. Supplier will ensure that its Personnel do not hold themselves out as employees or agents of Citi, nor seek to be treated as employees of Citi for any purpose, including claims of entitlement to fringe benefits provided by Citi, or for disability income, social security taxes or benefits, Federal unemployment taxes, State unemployment insurance benefits or Federal income tax withholding. Supplier is solely responsible for all employer-related responsibilities with respect to its Personnel including, but not limited to maintaining all required insurance coverages, filing all applicable tax returns and making all required payments and deposits of taxes in a manner consistent with Supplier’s status as an independent contractor.
7.2 Replacement of Supplier’s Personnel

Supplier will remove and replace any Personnel assigned by Supplier to a Project if Citi notifies Supplier that he or she is unacceptable to Citi for any other non-discriminatory reason. Supplier further agrees to remove and replace any Personnel assigned to a Project and to bar him or her from providing Services to Citi (or from any responsibility with respect to the delivery or oversight of Services) immediately where he or she is unable or unwilling to provide the Services in a timely and professional manner.

7.3 Supplier’s Personnel Policies

Supplier represents, warrants and covenants that it maintains and effectively administers comprehensive policies and procedures for qualifying its Personnel who are natural persons and are assigned to provide onsite Services to Citi, and that those policies and procedures include work authorization verification, background checks of employment history and criminal convictions, as further set forth herein, and pre-employment drug testing, all to the extent permitted by Applicable Law and any applicable collective bargaining agreement. Without limiting the generality of the foregoing, Supplier further represents, warrants and covenants that it has controls and procedures to ensure Supplier’s full compliance with all immigration-related Applicable Law, including validating that all Supplier Personnel assigned to Citi are authorized to work throughout the assignment in full compliance with all immigration-related Applicable Law. Upon request, Supplier will promptly provide Citi with written evidence of work authorization for any or all Supplier Personnel assigned to Citi and its compliance with immigration-related Applicable Law and will replace any Personnel that does not have work authorization consistent with Applicable Law with suitably qualified replacements, including providing all necessary training and orientation to ensure the timely and effective provision of Services, in each case at no additional cost.

8 FRAUD MANAGEMENT

8.1 In connection with Citi’s efforts to identify and mitigate fraud risk (“Fraud Management”), All Suppliers shall:

1. Cooperate with any Citi investigation of suspected or alleged theft, fraud or other potential criminal activity or wrongdoing, and any prosecution of fraudulent or criminal behavior to the fullest extent of the law;
2. 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 nonemployee (e.g., temporary employees and contractors);
3. Permit monitoring and oversight by Citi and its representatives and support Citi – and Law Enforcement – led investigations into potential fraudulent activity involving that Supplier;

4. Report, in a timely manner, any conflict of interests (including conflicts of interests between Suppliers/Supplier Employees and/or Citi Employees) of which Suppliers are made aware; and

5. Support Citi’s fraud-prevention processes during the set-up or update of a Supplier’s bank account in Citi’s Supplier payment system.

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

1. 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;

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

3. 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).

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

1. 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.

2. have connectivity to Citi networks / systems; and

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

   a) Identification, on-boarding or processing applications from new clients;

   b) Citi or Client Payment / Fund Transfer activities, and / or authentication of Citi clients access these services;

   c) Making, checking or fulfilling changes to Citi data or Citi-client (e.g., demographic) data;

   d) Provision, servicing or authorization of transactional instruments (e.g., debit / credit cards, eWallets, chequebooks, etc.);

   e) Provision or support of operational fraud management activities to Citi, relating to the prevention, detection or response to fraud events;

   f) Providing physical access to cash, financial instruments and assets / physical goods;

   g) Unescorted or off hours access in Citi facilities;

   h) Financial Statements: accounting activities, such as posting entries to the GL / SL;

   i) Earning and spending Rewards for incentivized activities.
9 MEDIA INTERACTION AND PUBLIC APPEARANCES

Citi Enterprise Services and 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. 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.

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), conduct or 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 the senior country or regional public affairs officer.

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.

10 WRITTEN ELECTRONIC COMMUNICATIONS

When interacting with Citi personnel, or in the performance of its obligations for or on behalf of Citi, Suppliers are permitted to use only those Written Electronic Communications Equipment, Systems and Services that approved by Citi. New, expanded, or modified Citi eComm Channels, whether as standalone tools or integrated into a broader platform, Citi-provided or third-party, must be approved in accordance with applicable Citi Requirements of which Supplier has been notified in writing by their BAO. Communicating Citi business with Citi personnel on non-Citi approved messaging platforms, such as WhatsApp, WeChat, LINE, Slack, Signal, Telegram, iMessage, SMS, Viber, and any other interactive electronic platform, is prohibited.

Additionally, Suppliers should have no expectation of privacy with respect to written Electronic Communications created, discovered, used, accessed, downloaded, stored, transmitted, received or deleted via Citi-provided Communications Equipment, Systems and Services. Citi may monitor Electronic Communications Equipment, Systems and Services, and Electronic Communications. Such Electronic Communications are owned by Citi and may be retained in accordance with applicable record retention requirements (subject to local law and regulation).
For further information, review the Electronic Communications Policy.

11 POLITICAL ACTIVITIES AND CONTRIBUTIONS

A variety of laws, such as campaign finance, gifts and entertainment, legislative and regulatory lobbying, procurement, pay-to-play, and securities, regulate political activities, including disclosure requirements, of Citi and its Suppliers. Any political activity by Suppliers that does not comply with relevant Citi policy or standards, law or regulation is prohibited.

**Political activity includes but is not limited to:**

1. Making corporate or personal political contributions, soliciting political contributions, using company 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;
2. 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
3. Seeking, accepting or holding any political office associated with a government, including any government board, commission or other similar organization.

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 Global Operations Control (ggaccontrol@citi.com). Although Citi may pay a fee and/or reimburse out of pocket costs for contracted and permissible political activity services provided by the Supplier, such as lobbying, Citi will never reimburse a Supplier or any of its employees for personal or corporate political contributions of any kind.

12 ANTI-MONEY LAUNDERING (“AML”)

**12.1 AML-Related Obligations:**

1. Maintain and comply with Citi processes and procedures designed to address the requirements of applicable laws, including (i) the Gramm-Leach-Bliley Act and the regulations promulgated thereunder; (ii) the USA PATRIOT Act and the regulations promulgated thereunder; (iii) any law or regulation addressing
money laundering; and (iv) any law or regulation related to economic sanctions. Such policies and procedures will address anti-money laundering roles and responsibilities, including the requirements to promptly report any observed activity that appears unusual or potentially unusual related to the intake of cash; and

2. Ensure that those of its Personnel providing Services to Citi receive annual training with respect to anti-money laundering roles and responsibilities, including the requirements to promptly report any observed activity that appears unusual or potentially unusual related to the intake of cash. The training may include such components as:
   a. Reporting and escalation of suspicious activity
   b. A “Know Your Customer” program, including a Customer Identification Program, sanctions and name screening, customer due diligence and enhanced due diligence
   c. Transaction monitoring
   d. Periodic reporting/metrics, including reporting on legal and regulatory changes and material AML program changes
   e. Testing and controls of AML program effectiveness, including site visits

3. Comply with any Contract provisions that define any AML program that must be instituted by the Supplier.

4. Promptly report to Citi in writing any suspected breaches of law, including any observed activity that appears unusual or potentially unusual related to the intake of cash related to Citi or its customers.

5. Comply with all applicable tax laws and regulations in the countries where they operate. Under no circumstances should suppliers engage in deliberate illegal tax evasion or facilitate such evasion on behalf of others, which may include engaging in activities that would assist in evading the payment of taxes that are due and payable or concealing information from tax authorities. As such, Suppliers shall adopt reasonable prevention procedures relating to tax evasion and promptly report to Citi in writing any violations or suspected violations that relate to Citi.

12.2 Suppliers shall maintain appropriate internal policies and procedures to comply with all AML laws and regulations now in existence or hereinafter brought into effect.
Supplier must work with their primary Citi business contact or BAO to ensure the Records Inventory identifies and classifies 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 and information that have met the retention obligation listed in the MRC and not subject to Record Hold, must be disposed of within one year of becoming eligible for disposition. Records subject to General Data Protection Regulation (GDPR) must be disposed of within 6 months of becoming eligible for disposition, unless subject to Record Hold. 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 unless subject to Hold. Supplier shall check with their primary Citi business contact or the BAO in the event of any uncertainty.

Suppliers maintaining documents on behalf of Citi are responsible for preserving (“holding”), collecting, and producing all Information that is deemed to be relevant to a legal or other proceeding within the required time as requested to them by the BAO.

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. Records Management and 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 to review and update contact names, procedural details, roles and responsibilities and the Supplier Record Inventory.

14 CUSTOMER-FACING SERVICES

Applicable to Supplier interacts with any individual in such individual’s capacity as a past, current, or potential customer of Citi or of a related party (such as an employee or a representative) of such customer (each such individual, a “Customer”).

14.1 Working Hours
Supplier shall instruct, and use reasonable efforts to ensure that, those of its Personnel working on Citi’s facilities do not attempt to gain access to Citi’s facilities outside of normal working hours (or on a scheduled holiday) for those facilities and to cooperate with, and comply with the security-related instructions of, Citi’s Personnel.

14.2 Policies and Procedures
With respect to Customer-Facing Services only: Supplier acknowledges and agrees that its commitment, under any Contract, to have those of its Personnel working on Citi’s facilities comply with Citi’s workplace policies and procedures includes compliance with the physical security procedures and other security measures of Citi and its Affiliates. Citi
will use reasonable efforts to keep Supplier apprised of all physical security procedures and other security measures. Citi will have the discretion to issue, activate, confiscate and deactivate identifications cards, keys or other security devices to or from those of Supplier’s Personnel working on Citi’s facilities; provided that Citi’s conducting of these actions will not be deemed to imply any employment relationship between Citi and such Personnel.

14.3 Disaster Recovery Plan

Supplier will maintain a contingency plan (a “Disaster Recovery Plan”) for the continuation of business (and provide evidence of its current and periodic testing, if requested by Citi) so that despite any disruption in Supplier’s ability to provide the Services or to perform its other obligations hereunder from any particular location or through the efforts of any particular individuals, Supplier will promptly be able to provide the Services and perform its obligations from an alternate location or with replacement Personnel. A copy of the Disaster Recovery Plan must be provided to Citi within ten (10) calendar days of the Effective Date of each Work Order entered into between Citi and Supplier for Customer-Facing Services, and annually thereafter for so long as each Work Order is in effect. Supplier will provide Citi with any instructions or other information necessary for Citi to continue to receive Services from Supplier under circumstances where Supplier has had to invoke its Disaster Recovery Plan. Supplier represents, warrants, and covenants that its disaster recovery plan will, at a minimum, include:

1. Maintenance by Supplier of a secondary disaster recovery site separate from the Service locations, the storing of back-up media at a location separate from the Service locations, the use of redundant communications lines and servers, etc.;
2. Procedures for back-up/restoration of operating and application of the Services, including a detailed, documented plan for responding to a prolonged disruption in Services caused by power failure, system failure, natural disaster, or other unforeseen circumstances that includes processes and procedures for resuming operations within a mutually agreed upon time period;
3. Procedures for the protection of all Content;
4. Procedures and any third party agreements for replacement equipment (e.g., computer equipment), and
5. Procedures for any off-site production facilities. In addition, Supplier’s Disaster Recovery plan will provide that:
   a) Supplier will notify Citi in writing within two (2) hours of any disaster that could negatively impact the Services;
   b) Supplier will provide Citi, within 24 hours of said notice, a plan to continue to provide the Services at an alternative processing facility, and
   c) the Services must be fully operational within 48 hours of the initial notice. Supplier agrees, upon request, to release the information necessary to allow Citi to develop a disaster recovery plan and a continuity of business plan, which will work in concert with Supplier’s disaster recovery plan and continuity of business plan. Supplier agrees to annually test its disaster recovery plan and, upon request, provide a
written report of the results of the disaster recovery test to Citi. In the event that parts of Supplier’s facilities are inoperable, Supplier will treat Citi no less favorably than Supplier treats its other commercial customers. Supplier will ensure that any Subcontractor of Supplier maintains a Disaster Recovery Plan and related processes and controls that are fully consistent with the provisions and requirements of this Section.

14.4 Diligence Certificate.
Supplier acknowledges that Citi and its Affiliates are required to conduct regular diligence of those of its suppliers that conduct Customer-Facing Services through an annual questionnaire/certificate (the “Diligence Certificate”) that addresses:

a) Supplier’s business licenses (including articles of incorporation, certificates of good standing any applicable required licenses),
b) Supplier’s compliance with Applicable Law,
c) Insurance coverage,
d) Skills, qualifications, and expertise,
e) Supplier’s capacity (including staffing levels and workload balancing),
f) Relevant Business processes,
g) Compensation practices,
h) Financial viability and counterparty risk,
i) Reputation risk (complaints / pending litigation),
j) Customer-facing policies and practices,
k) Supplier’s references,
l) relationship of principals,
m) reliance on subcontractors, contractors or any third-party providers,
n) training program review,
o) business continuity plan,
p) quality audit results and compliance with any applicable service level commitments, and
q) document management and storage.

Supplier will, from time to time, provide Citi with any other information or documents as Citi may request in order to ensure compliance with (i) any Contract, (ii) Citi’s corporate policies, and (iii) regulatory requirements applicable to Citi and Supplier.

14.5 Customer Complaints.
Supplier will notify their primary Citi business contact (or designee) in writing within twenty-four (24) hours of any written or oral submission of dissatisfaction or concern (each, a “Complaint”) received by Supplier from any Customer or from any Regulator related to the Services provided by Supplier on Citi’s behalf, or otherwise related to Citi including any Complaint related to the possession or use of Customer Data or the Customer’s privacy rights. Unless Citi makes such a system available to Supplier, Supplier will also develop, implement, and maintain a system (“Tracking System”) reasonably satisfactory to Citi to
track Complaints and provide Citi, at its discretion, a copy of reports or access to systems. The Tracking System will:

1. categorize Complaints by type, date received, and date notice of the Complaint was provided to Citi,
2. track the course of handling of the Complaint until conclusion/resolution, and
3. provide for all other matters as may be reasonably requested by Citi. The Tracking System must be designed to allow Supplier to determine if it receives an inordinate number of Complaints regarding a particular matter so that Supplier (in consultation with Citi) can determine if there is a systemic issue regarding Supplier’s business or its provision of Services and promptly correct problems.

14.6 Network and Communications Security

Deploy multiple layers of defense including on Supplier systems, but not limited to firewalls, network intrusion detection, and host-based intrusion detection systems. All security monitoring systems including, but not limited to, firewalls and intrusion detection systems must be monitored 24 hours per day, 365 calendar days per year. Configure firewalls, network routers, switches, load balancers, name servers, mail servers, and other network components in accordance with commercially reasonable industry standards. At the request of Citi, based on information received by Citi about vulnerabilities and threats, restrict access to any Citi-specific component of the networks, systems, and applications used to provide services under any Contract.

14.7 Physical Security

Maintain all workstations, servers, and network equipment used to provide services under any Contract in secure facilities owned, operated, or contracted for by Supplier. Limit access to these secure facilities to authorized Supplier staff members with job-related needs. Monitor access to these secure facilities through the use of security guards, surveillance cameras, authorized entry systems, or similar methods capable of recording entry and exit information. Maintain all backup and archival media containing Citi information, or other information used to provide services under any Contract, in secure, environmentally-controlled storage areas owned, operated, or contracted for by Supplier. Limit access to backup and archival media storage areas and contents to authorized Supplier staff members with job-related needs.

14.8 Business Continuity and Recovery

Perform backups of all systems, applications, and data used to provide services under any Contract in a manner consistent with the business resumption specified elsewhere in any Contract.

14.9 Regional Service Level Standards
Each Region is responsible for resolving and responding to Complaints/Concerns in a timely manner. Please see your Regional standards/procedures that include implementation and definition of Service Level Standards. Covered Businesses will calculate timeliness with the following start dates:

1. For phone and personal interactions, the Service Level Standard begins on the date the Complaint/Concern was received by the organization.
2. For written and electronic communications and social media, the Service Level Standard begins on the date the dissatisfaction was detected.

14.10 Call Recording and Call Retention

Suppliers must implement a process for recording and storage of all calls related to Complaints / Concerns that are handled in Call Centers by employees, and their direct managers, whose primary role is to speak with consumers for at least 12 months from the date of the call unless otherwise directed by local regulatory requirements. Periodically transfer backup media to a secure off-site storage facility.

15 ENTERPRISE RESILIENCE / CONTINUITY OF BUSINESS

Applicable to Suppliers who are included in the Recovery Plan for the Citi Business unit or if the supplier hosts an application with recovery capabilities (i.e., numeric Technology Recovery Time Capability (TRTC) or Recovery Time Objective (RTO), which is used by Citi. The Citi Business (BAO) is responsible for communicating applicability and COB requirements to the Supplier

15.1 Recovery Resources. Suppliers' Disaster Recovery Plan must provide alternate resources capable of delivering all products and services to Citi in the event 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.

1. 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.
2. Suppliers of Software as a Service (SaaS) applications hosted at Cloud Service Providers (CSP), geographical separation requires distinct CSP Regions for the primary and CoB / disaster recovery environments

15.2 Recovery Service Levels. Suppliers' business continuity must meet established levels of service in order to be effective for Citi. At minimum, Supplier's Disaster Recovery Plan shall establish specific values for:

1. Recovery Time Objective
2. Recovery Point Objective
3. Recovery Resources / Technology Capacity
4. Recovery Duration
15.3 Disaster Recovery Plan. Supplier will maintain a Disaster Recovery Plan for the continuation of business (and provide evidence of its current and periodic testing, if requested by Citi) so that despite any disruption in Supplier’s ability to provide the Products/Services or to perform its other obligations hereunder from any particular location or through the efforts of any particular individuals, Supplier will promptly be able to provide the Products/Services and perform its obligations from an alternate location or with replacement Personnel. A copy of the Disaster Recovery Plan must be provided to Citi within ten (10) calendar days of the Effective Date of each Work Order entered into between Citi and Supplier, and annually thereafter for so long as each Work Order is in effect. Supplier will provide Citi with any instructions or other information necessary for Citi to continue to receive Products/Services from Supplier under circumstances where Supplier has had to invoke its Disaster Recovery Plan. Supplier represents, warrants, and covenants that its disaster recovery plan will, at a minimum, include:

1. Recovery procedures and strategies, including relocate, transfer of work, and/or remote access to mitigate the effects of disruptions including unavailability of technology (Denial of Service/DoS), unavailability of primary work location (Denial of Access/DoA), and unavailability of staff (inclusive of subcontractors);
2. Maintenance by Supplier (including but not limited to) of a secondary disaster recovery site separate from the Product/Service locations, the storing of back-up media at a location separate from the Product/Service locations, the use of redundant communications lines and servers;
3. Procedures for back-up/restoration of operating and application of the Products/Services, including a detailed, documented plan for responding to a prolonged disruption in Products/Services caused by power failure, system failure, natural disaster, or other unforeseen circumstances that includes processes and procedures for resuming operations within a mutually agreed upon time period;
4. Procedures for the protection of all Content;
5. Procedures and any third party agreements for replacement equipment (e.g., computer equipment);
6. Procedures for any off-site production facilities; and
7. Supplier’s Disaster Recovery plan will provide that:
   a. Supplier will promptly notify Citi of any disaster that could negatively impact the Products/Services;
   b. Supplier will provide Citi, within 24 hours of said notice, a plan to continue to provide the Products/Services at an alternative processing facility;
   c. The Products/Services must be fully operational within the required Recovery Time Objective (RTO), 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”; and
d. In the event that parts of Supplier’s facilities are inoperable, Supplier will treat Citi no less favorably than Supplier treats its other commercial customers.

15.4 Disaster Recovery Plan Requirements Applicable to Hosted Services. To the extent Supplier manages and provides a Hosted Service to Citi, the provisions that follow shall also apply. The Disaster Recovery Plan will, at a minimum, include:

1. Procedures for back-up/restoration of operating and application of the Hosted Services, including a detailed, documented plan for responding to a prolonged disruption in services caused by power failure, system failure, natural disaster, or other unforeseen circumstances that includes processes and procedures for resuming operations within a mutually agreed upon time period;
2. In addition, Supplier’s Disaster Recovery Plan will provide that: (a) Supplier will notify Citi in writing within two (2) hours of any disaster that could negatively impact the Hosted Services; (b) Supplier will provide Citi, within 24 hours of such notice, a plan to continue to provide the Hosted Services at an alternative processing facility, and (c) the Hosted Services must be fully operational within 48 hours of the initial notice;
3. Supplier agrees, upon request, to release the information necessary to allow Citi to develop a disaster recovery plan and a continuity of business plan, which will work in concert with Supplier’s disaster recovery plan and continuity of business plan; and
4. In the event that parts of Supplier’s facilities are inoperable, Supplier will treat Citi no less favorably than Supplier treats its other commercial customers.

15.5 Changes to the Disaster Recovery Plan. Supplier may change its Disaster Recovery Plan as long as the changes do not degrade the Disaster Recovery Plan in a manner that is likely to adversely affect the services (e.g., lengthening its RTOs). Supplier will promptly communicate any changes in its Disaster Recovery Plan to Citi and, at Citi’s request, explain changes so that Citi will fully understand and be able to respond to the changes.

15.6 Subcontractors’ Disaster Recovery Plan. Supplier will ensure that any Subcontractor of Supplier maintains a Disaster Recovery Plan that is fully consistent with the Citi Requirements for Suppliers.

15.7 Disaster Recovery Plan Invocation and Crisis Notification. Suppliers will promptly notify the primary Citi business contact:

1. when Supplier invokes its Disaster Recovery Plan; and;
2. concerning any crisis, threat, warning or cyber event against Supplier or its subcontractors that is reasonably likely to have an adverse impact on the services or products provided to Citi.

15.8 Testing. All the Supplier’s recovery resources and plans must test within 120 days following production implementation and be tested annually (every 12 months) at minimum. Testing shall demonstrate the Supplier’s ability to meet the recovery service levels for all products and services delivered to Citi. In the case of Suppliers of SaaS applications hosted at Cloud Service Providers (CSP), failover tests must be conducted between production and recovery environments located in distinct CSP Regions dedicated and/or designated for Citi (e.g., US-East1 and US-East 2 or US-East1 and US-West1). These tests must be comprehensive and include the full scope of Services provided to Citi. Suppliers must provide Citi with at least 30 calendar days’ advance notice of testing the recovery of products/services provided to Citi. Citi may participate in or observe Supplier’s recovery testing. If Citi wishes to participate, Supplier will provide Citi with the test objectives, the test plan, and procedures for connecting to the test site before conducting the test. Within ten (10) business calendar days after completing each test, Supplier will provide Citi with a summary of the test objectives, the test plan and the test results, including the timeframes required to recover critical business functions and evidence of the test results (e.g., screen shots).

For Denial of Access (DOA) tests (Unavailability of Primary Work Location):

1. Processes Most Critical to the Citi Franchise. Citi will participate in or observe Supplier’s testing activity for all processes that it has defined as “Franchise Critical”. For such processes, 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. 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.

For Denial of Service (DOS) tests (Unavailability of Technology):

1. Applications included in a Citi Business Recovery Plan. Citi will participate in or observe Supplier’s testing activity for all applications. During the test, Citi staff will participate to validate the application’s functionality in the Supplier’s recovery environment. Supplier permits Citi to review recovery plans covering technology, test scripts, test results, and evidence.

2. Applications not included in a Citi Business Recovery Plan. Citi need not participate/observe Supplier’s testing activity. Supplier will provide recovery plans covering technology, test scripts, test results, and evidence.
15.9 Volume Validation. A Supplier that hosts Citi’s Franchise Critical Applications (FCAs) used for critical transaction processing must demonstrate that Production volumes can be processed in their CoB / disaster recovery environment. Citi and the Supplier must agree on the methodology to be used for validation.

15.10 Use of Citi’s Systems to Provide Services. If requested by Citi or Citi’s Affiliates, Suppliers using Citi’s Systems will participate, at no cost or charge to Citi, in Citi’s disaster recovery exercises.

15.11 Addressing Test 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).

15.12 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 a 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.

15.13 Assessments. Suppliers are subject to Citi’s Third-Party CoB Assessment Process for assessing business continuity capabilities commensurate with Citi’s Process Criticality / RTO:

1. Suppliers supporting processes with an RTO <= 24 hours must be assessed on an annual basis
2. Assessments for Suppliers supporting Franchise Critical processes must be conducted at the Supplier’s site
3. Suppliers supporting processes with an RTO > 24 & <= 72 hours do not require an assessment to be performed but must attest to their recovery capabilities annually
4. The assessment will consist of business recovery questionnaires requiring responses from Supplier with evidence. Should the findings of a CoB Assessment identify or indicate issues or concerns, Citi will document findings in a notice to Supplier and work with Supplier to identify means for correcting the problems.

15.14 Operational Resilience. Critical Business Services are those services which, if delivery was disrupted, could cause significant adverse impact to Citi, its clients or the financial system. Supplier shall ensure that any disruption to the delivery of elements of the services that either amount to critical business services or support the provision of critical business services by Citi, as specified by Citi from time to time (“Critical Business Services”) does not exceed the duration set by Citi or otherwise breach any
relevant metric set by Citi (“Impact Tolerances” as notified to Supplier from time to time.

Impact Tolerances will be expressed as a clear metric, including a maximum tolerable duration or Maximum Tolerable Downtime (MTD) for which delivery of the Critical Business Service may be disrupted. Citi and Supplier shall review the Impact Tolerances annually as part of the ongoing contract governance processes. Where Citi is required to set two Impact Tolerances for an individual Critical Business Service due to the requirements of more than one Regulatory Body, then Citi may specify separate Impact Tolerances for such Critical Business Service. Supplier shall:

1. Notify Citi as soon as it becomes aware that it has failed (or is reasonably likely to fail) to deliver any Critical Business Service within the corresponding Impact Tolerance(s) set by Citi together with an explanation of the reasons for any prospective or actual failure and the steps being taken to mitigate the impact of such failure;
2. Where requested to do so, provide reasonable assistance to Citi to enable it to identify the people, processes, technology, facilities and information that are necessary for Supplier to deliver any Critical Business Services;
3. Reasonable assistance to Citi for the purposes of enabling Citi to conduct:
   a. any internal scenario testing of Supplier’s ability to remain within the Impact Tolerance(s) for each Critical Business Service in the event of a severe but plausible disruption to its or the Supplier’s operations; and
   b. any lessons learned exercised following a scenario test to enable Citi to identify weaknesses and any actions necessary to improve Supplier’s ability to effectively respond and recover from future disruptions.
4. Where any internal scenario testing by Citi identifies vulnerabilities or limitations on Supplier’s ability to deliver Critical Business Services within the corresponding Impact Tolerance(s) set by Citi and following any failure by Supplier to deliver any Critical Business Service within the corresponding Impact Tolerance(s) set by Citi, the parties will agree a plan (including a timetable to implement the plan), to ensure that Supplier takes the steps necessary to resolve or mitigate such vulnerabilities or limitations or remedy the cause of the failure to remain within the Impact Tolerance(s) (as applicable) as soon as is reasonably practicable.
16 GLOBAL BACKGROUND SCREENING STANDARDS

Applicable to Suppliers whose personnel has access to Citi systems/networks AND/OR unescorted access to Citi premises AND/OR utilize Subcontractors. (Such personnel would be required to have a GEID, and be registered in Citi’s Non-Employee Management System)

16.1 Overview – Background Screening

Background screening must be performed in accordance with all applicable local laws and regulations. All information and self-disclosures described within this document must be provided by Supplier’s personnel and Subcontractors 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.

Additional information on background screening completion timing, country-specific requirements and exceptions to these standards can be found at https://www.citigroup.com/citi/suppliers/data/country_background_screening_requirements_tables.pdf.

16.2 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 email 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.

16.3 Sanctions Screening

All Supplier personnel, including Subcontractors irrespective of access to Citi data/systems/networks AND/OR access to Citi premises, 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”). Screening must apply to 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.

OFAC lists are publicly available at this website: https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists
16.4 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.

16.5 Employment History
Suppliers must validate the employment history of its personnel for the past seven (7) years or 10 years if required per regulation. 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.

16.6 Education History
Suppliers must 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.

16.7 Criminal Background
Where legally permissible, Suppliers’ personnel and sub-contractors must disclose to Citi if they become subject to an arrest, summons, subpoena, arraignment, indictment or conviction for any criminal offense, including a guilty plea or no contest plea and any participation in a pre-trial diversion or similar program. The administrative review of criminal records and / or fingerprint checks must be completed 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.

16.8 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 country-specific requirements and exceptions located https://citigroup.com/citi/suppliers/data/country_background_screening_requirements_tables.pdf.
16.9 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.

17 EXPENSES

Suppliers that are contractually eligible to claim reimbursable business expenses.

17.1 Overview

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, are in accordance with the terms of the applicable Contract or Citi’s Expense Management Policy, where appropriate, and are adequately substantiated through supporting receipts, invoices, itineraries, or other forms of documentation as deemed acceptable by Citi.

17.2 Reimbursements

These expenses must be properly documented and invoiced to Citi in accordance with Citi invoicing requirements. Supplier expenses must not be incurred by a Citi employee on behalf of a Supplier. Any expense submitted to Citi for reimbursement of a valid and approved expense item(s) must include (in addition to all other invoicing requirements):

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

For information on permissible reimbursable business expenses, please contact your primary Citi business contact. Supporting receipts, invoices, itineraries, or other forms of documentation as deemed acceptable by Citi must be submitted with the reimbursement claim. Reimbursement claims must be compliant with the provisions in the applicable Contract or with Citi’s Expense Management Policy, where appropriate, and approved by the appropriate business sponsor and / or primary Citi business contact and approved by an individual who has been duly authorized and has a sufficient amount for the corresponding commodity. Non-compliant requests will not be reimbursed.
18 INFORMATION SECURITY (IS)

Applicable to Suppliers including Subcontractors that access, process, store, or manage any Citi Information as classified and defined in the Appendix; or Host Citi branded Internet-facing applications; or have connectivity to Citi’s network resources; or require unescorted access to Citi facilities.

18.1 Overview.
This Section provides minimum requirements for Citi’s Suppliers, including Subcontractors, who store, process, manage, or access Citi Information or host Citi applications, regarding the information protection controls that are expected by Citi. These requirements ensure that information is protected in accordance with applicable legal and regulatory requirements and the highest industry standards (e.g., ISO / IEC 27002) in the locations where Citi and its Suppliers do business. If local laws, regulations, or relevant industry standards establish higher standards 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 contractual terms and conditions. If a Supplier decides to implement additional security practices or procedures for information security, the Supplier must ensure that those practices and procedures do not conflict with the minimum controls defined in this section.

18.2 Information Security Policy & Governance.

Suppliers must have documented information security policies and standards. The policy governance must include clearly defined roles and responsibilities and annual policy and standard review/update for consistency with the current state of technology, industry standards, legal, and regulatory requirements.

1. Segregation of Duties. Supplier must have processes in place ensuring 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.

18.3 Exceptions.

1. 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.
2. 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 or higher information.
3. 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.

4. A person who needs to update production data outside of application controls must use temporary privileged access.

5. A person who needs to view data containing Confidential PII or Sensitive PII data outside of application controls must use temporary privileged access.

6. Individuals performing the Develop or Certify function must not modify or install operating system or database infrastructure software in Controlled Information Systems.

18.4 Management Commitment to Information Security.

Suppliers, who will host a Citi-branded Internet-facing application or have access to Citi Information with 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 requirements and any legal and / or regulatory requirements (applicable to either Citi or Supplier) that pertain to information security.

The assessment consists of security questionnaires requiring responses from the Supplier with supporting evidence and may include visits to Supplier’s locations where Citi’s Confidential or higher Information may be stored, processed, managed, or accessed by the third-party. Should the findings of a TPISA disclose or indicate security problems or concerns, Citi will document findings in a notice to the Supplier and work with the Supplier to identify a means for correcting the problems. Suppliers must expeditiously make the necessary corrections add / or compensating controls to address Citi’s concerns to Citi’s satisfaction and meet required timelines of 180 calendar days for High-Risk issues, 240 calendar days for Medium Risk issues, and prior to the next assessment for Low-Risk issues.

1. The Supplier must regularly perform assessments of its business operations and related controls against its own information security standards, policies, and procedures. The periodic assessments must include, at a minimum:

   a) Assessment of the processes the Supplier uses to ensure compliance with the Supplier’s own IS policy and standards;

   b) 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 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.

2. Issues that have been identified as a result of any Information Security Risk Assessment must be documented and tracked to closure with evidence of remediation provided to Citi.
3. If the Supplier’s Information Security management function is relocated across country borders, the Supplier must obtain Citi’s documented approval prior to such relocation.

4. If the Supplier acquires a new entity, the Supplier must complete an assessment of the acquired entity for compliance with these Standards.

5. 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.

6. If Supplier hosts software or a website that contains Citi Information or is Citi branded, periodic vulnerability assessments must be performed in accordance with Citi’s System Security Testing Standard (SSTS) and any material issues identified during the assessment must be remediated within the timeframes specified in that Standard. As the SSTS is not approved for external distribution, Suppliers must work with their Citi Relationship Manager to ensure compliance with the reference documentation. In addition, the Supplier must comply with relevant ISO/IEC 27001 Information Security management standards (or successor information security management standards that establish higher standards and protocols) and abide by the information security provisions contained within this Section (18).

7. If connectivity to servers and / or Information Systems on the Citi internal network is required, then the Supplier is required to notify their primary Citi business contact so that the current connectivity provisioning process can be followed.

8. The Supplier must promptly notify the appropriate Citi contact (Business Activity Owner (BAO) of any unauthorized access, acquisition, loss, corruption, or deletion of Citi Information or any other compromise to Information Systems used to store, process, or transmit Citi Information.

9. The Supplier must ensure that all high-risk activity or changes to sensitive data have audit trails that enable specification of what individual performed what activity or changed what data.

10. The Supplier must ensure that all sensitive data is masked on screen and on paper, including, for example, monitoring, exception, regulatory, and other reports).

11. The Supplier must restrict printing, recording, or copying of sensitive data, including by its own devices. Supplier must perform all reasonable efforts to return or destroy all Citi information at an agreed upon point in time during or at the end of the agreement.

12. The Supplier must ensure all supplier personnel (employees, contractors, temps, subcontractors) with access to Citi information sign a non-disclosure or confidentiality agreement (NDA).

13. The Supplier’s employees must be provided an employee handbook, or similar document that contain disciplinary process for non-compliance with violations of the Supplier’s code of conduct and human resources policies that must be acknowledged as part of their onboarding process.

14. The Supplier has a process in place to retrieve all assets when an employee or nonemployee is terminated or resigns.
18.5 Subcontractor Information Security Risk.

The supplier must require that subcontractors with access to their client's data require pre-contract and periodic post contract Information Security (IS) assessments performed by qualified Information Security personnel that includes:

1. A management approved subcontractor Information Security assessment process is in place, and it covers all steps from assessment initiation through issue management.
2. Suppliers ensure IS risk assessments are performed on their subcontractors that have access to Citi Confidential and higher data using an IS assessment questionnaire or equivalent tool that covers IS domains that align with those covered in Citi's Third Party IS Assessment Questionnaire (TPAQ) and includes a logical method for calculating Information Security risk as it relates to sub-contractors.
3. Suppliers ensure they assess the IS controls of sub-contractors with access to Citi Information, track assessment completions, and manage the noted issues and corrective action plans (CAPs) to closure.

18.6 Responsibility 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. Supplier must be responsible for protecting all Citi Information under its control.
4. Supplier must ensure accountability of its users' activity in a manner consistent with industry practices.
5. User access to personal external Internet e-mail storage and cloud storage accounts must be restricted from the Supplier's global network where Citi Information resides.

18.7 Information Classification & Handling.

Citi classifies information per the following Information Classification table below. See the Appendix for definitions and examples of each information classification listed below.
1. Based upon the classification of Citi Information, Citi must work with the Supplier to specify the level of security required to protect such information and Supplier must ensure that sufficient controls are in place, along with any heightened or modified levels that Citi may require.

2. Confidential or higher information must be stored on 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. If the Supplier allows the use of non-company owned devices to store Citi data (i.e., devices managed by a 4th party), the Supplier must have a policy in place that requires specific management approval and have established guidelines and monitoring procedures for the use and disposal of Citi Information.

4. Only information classified by Citi as Public may be stored on Supplier personnel-owned devices (e.g., home computers, personal digital assistants, and mobile Internet and email applications).

5. Supplier must always protect Citi Information from unauthorized access, modification, or deletion.

6. 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.

18.8 Secure Configuration

1. The supplier is required to maintain a documented secure configuration standard for all assets with the potential to store, process, access, or transmit Citi Information.

2. Supplier must incorporate information security controls in its processes and procedures for the selection, development, and implementation of applications, products, and services.

3. Supplier must have a secure build procedure for all systems where Citi Information is stored, processed and/or transmitted.

4. Supplier must maintain a secure image or template for all systems.

5. All default user accounts and passwords must be removed and/or changed from vendor-supported systems, network devices, and applications.

6. Any system or service that has been compromised must be re-built and configured using image or template that has a proven integrity.
7. Any change to be made to a secure configuration must be approved by management via a change management process.
8. When changes occur to the secure configuration, a notification process must be in place that includes follow up and corrections.
9. The secure build procedure must include tools to support automated configuration checks of the security / standard build settings at the time of production deployment.

18.9 Encryption Requirements.

When a Third Party transmits and stores Citi Information classified as Confidential or higher, encryption requirements must be followed. Data transmitted between Citi and the Citi Third Party must be encrypted end-to-end with Citi approved tools or solutions. Approved protocols and respective version numbers during transmission of data are as follows:

1. When exchanging authentication and authorization information: SAML v2.0, OAuth v2.0 (authorization only),
2. To protect the communication channels and the associated exchange of keys the following Network Security Protocols are permitted:
   a) TLS v1.3 - All TLS v1.3 suites are permitted. If TLS 1.3 is the only permitted protocol, no additional review is necessary.
   b) TLS v1.2 - If TLS 1.2 is permitted, then a grade of B or higher from SSL Labs is acceptable and no additional review is necessary.

Data persistently stored in the Citi Third Party environment or when exchanged must be fully encrypted using Citi approved tools or solutions. Approved algorithms and key lengths for encrypting data are as follows:

1. **Advanced Encryption Standard (AES):** Approved key lengths: 256 or more bits. Restricted Modes: Electronic Codebook (ECB) mode is prohibited except where the amount of plaintext is less than or equal to the block length. Disk drive encryption: AES with 256-bit key is required. AES with a 128-bit key length is allowed as a TLS Cipher, however Citi is in the process of deprecating this as part of our post-quantum cryptography program.
2. **ChaCha20 (a stream cipher for associated use cases):** Approved key lengths: 128 or 256 bits, with 96-bit nonce and 32-bit block count or 64-bit nonce and 64-bit block count. Maximum data size: 16 petabytes.

Approved public key cryptosystems, key exchange, agreement mechanisms, message digest and key derivation functions, are as follows:

1. **Public Key Cryptosystems and minimum key length sizes:**
   b) Digital Signature Algorithm (DSA): 2048 bits. DSA must not be used to secure Citi data processed or stored outside of Citi.
   c) Elliptic Curve Digital Signature Algorithm (ECDSA): 256 bits and as specified in ANSI X9.62 with NIST recommended curves.
2. **Key Exchange and Agreement mechanisms and minimum key length sizes:**

3. **Message Digest Functions:** Creating an encryption key of a length greater than the number of random bits in the material used to generate the hash is prohibited.
   a) SHA-1 Acceptable only for non-digital signature applications. SHA-2 family, SHA-3 family and POLY-1305: Acceptable for all cryptographic hash-function applications.

4. **Password based Key Derivation Functions and minimum requirements:**
   a) PBKDF2: Minimum iteration count of 10000 with a salt of at least 16 bytes.
   b) HKDF: Must be salted, and the info input value must be included.
   c) SCRYPT: Minimum number of rounds/cost factor of 10. Use of NIST SP800-108 KDF for Stream Encryption is prohibited.

5. **Password hash functions and minimum requirements:**
   a) Bcrypt (for local storage of authentication material): Minimum number of rounds/cost factor of at least 10.

18.10 External Email

Encryption requirement for individual emails containing Citi Information with a Citi Information classification of Confidential or higher, 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)). The approved secure E-mail protocols are:

1. **Identify-Based Encryption (IBE)** features encrypted email and must be used only within Citi customer facing solutions and secure e-mail and eDelivery systems only.

2. **Mandatory TLS (MTLS)** features Session encryption (does not encrypt e-mail payload) and is for use with Vendors, partners and clients who have pre-negotiated arrangements for its use.

3. **Domain Keys Identified Mail (DKIM)** features source authentication and key management and is for use with vendors, partners, and clients.

18.11 Private networks

Private networks that are independently regulated by a recognized authority and meeting Financial Services Industry standards 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 those networks provide the necessary infrastructure to fully support encrypted transmissions.

---

1 ECDHE is preferred.
18.12 Voice and Fax.

Information with a Citi classification of Confidential or higher sent over fax or discussed on voice calls (including Voice Over IP [VOIP]) may be sent unencrypted. When required, Supplier must develop specific procedures and guidance to protect Confidential or higher information sent via these channels.

18.13 Key, Secrets and Certificate Management.

The term secure boundary used in this section refers to a Cryptographic Module Validation Program (CMVP), such as Federal Information Protection Standard (FIPS), validated boundary (FIPS 140-2/3 Level 2 is the minimum acceptable security level). (Other unique security boundary cases must be brought to the attention of Security Architecture council (SAC) for their advice and approval).

1. Latest Industry standard cryptographic algorithms and minimum key lengths must be implemented for encryption and signing. Supplier must provide assurance via change management process documentation followed actively by the supplier covering periodic oversight and upgradation process to ascertain that Industry recommended cryptographic algorithms and minimum key lengths are used at all times.

2. Citi Third Party must have a formal documented key, secret and certificate management life cycle process with controls in place to protect sensitive material from unauthorized use or exposure. All secrets and key lifecycle events must only occur within a secure boundary. All access to privileged and secure boundaries must be well documented as well. The Supplier must provide a sequence diagram for all the key lifecycle events highlighting the actors, entities and boundaries involved.

3. Keys must have a unique purpose and must never be used for any other purpose, such as for encrypting another company data or third party’s internal use or same encryption key used for disk encryption as well as data encryption or same encryption key used for payload encryption as well as database encryption.

4. For all cryptographic keys (symmetric or asymmetric), the private key or private key material (such as Initialization vectors, seed or part of a private key) must not be displayed in the clear text at any time. Private key or private key material (such as Initialization vectors, seed or part of a private key) must never leave the secure boundary with the exception to ephemeral keys such as dynamic session keys. If the design required the derivation of a private key or material to be transmitted between secure enclaves/privileged access boundaries, they must be transmitted in encrypted form only using a Key Encryption Key (KEK) via mutual TLS encrypted tunnels only (These unique cases must be brought to the attention of Security Architecture council (SAC) for their advice and approval). The KEK must never leave the privileged access secure boundary where it was generated in this case.

5. Key Encryption Key (KEK) must be split into two or more key components and be XORed before distributing and for manual key entry/loading. KEK must have adequate Access Controls Lists (ACLs) associated inside of the secure boundary such as CMVP validated modules and the KEK must never leave the secure boundary.
6. Human or Service or Automated Agent Access to Keystores or secure boundaries containing private keys or secrets or private key material (such as Initialization vectors), seed or part of a private key must be properly segregated with controls limiting access to authorized personal or systems only.

7. Every request to access the Keystores containing private or symmetric keys must be logged and documented with details like who, when and the purpose of the access for audit purposes.

8. Self-signed and wildcard certificates must not be used. Default SSL certificates must never be used.

9. Keys must have a defined cryptoperiod time span as suggested in the NIST SP800-57 part 1, revision 5: Change of key does not need to match the key expiration stated. Keys must be refreshed or rotated prior to expiration to accommodate periods of change, scheduling conflicts and system freezes.
   a) While replacing an expired certificate, re-use of the old asymmetric key pair is prohibited.

10. Wireless networks must be encrypted with industry standard encryption algorithms.

11. Suppliers utilizing any form of cryptographic mechanism must use industry standard key management tools and techniques.

18.14 Access Control Responsibility.

To protect all Controlled Information Systems used to store, access, manage, process, or transmit Citi Confidential or higher Information from unauthorized access, the supplier is responsible for enforcing the concept of Least Privilege, by limiting user entitlements to the minimum level of access required for each job function by managing the provisioning of logical access to all systems and applications; controls must be fully documented, auditable and grant least privilege.

1. Supplier is responsible for the access rights of all users in its organization.
2. Supplier must implement access controls that ensure users are granted only those privileges and entitlements strictly necessary to perform their function.
3. Supplier must implement a process to ensure that all default access capabilities are removed, disabled, or protected to prevent their unauthorized use.

18.15 User Access Management.

The supplier must manage the provisioning of logical access to systems and applications that process, store and/or transmit Citi Confidential or higher information. This includes:

1. Identification and inventory of approved authentication systems.
2. All access to Citi data requires approval from a manager or manager’s designee and the system owner.
3. A combination(s) of privileges/functions an individual user may not be provisioned because they present conflicts of interests or violation of maker-checker rules.
4. A monitoring process to oversee and manage the access rights granted/revoked to each user on the system. Low risk suppliers are exempt from this requirement.

18.16 User Identification and Authentication.

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. All users must be:

1. Uniquely identified or mapped to the technology platform by a User ID.
2. Authenticated to the technology platform using an approved authentication method - supplier should contact its primary business contact (BAO) for current approved methods.
3. 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 BAO for current approved methods.
4. Users require authentication for external connections: (See 18.27 Remote Access).

18.17 Temporary Privileged Access.

The supplier must maintain an inventory of all privileged and administrative accounts. The direct login to a privileged Functional ID must be granted through a temporary privileged access process. Privileged access to Controlled Information Systems must follow a Temporary Privileged Access Management process that includes documented password / account release procedures that:

1. Requires the requester to be on a pre-approved authorized users list or have an approval at the time of use.
2. Requires documented justification in a change/problem ticket before access is granted.
3. Includes an independent review of the activity performed with the access.
4. Includes a process to revoke / remove the access after a pre-defined period of no more than 24 hours.
5. Allows production and post-implementation stabilization access - such as after a major upgrade or break / fix resolution, to be extended up to seven (7) calendar days.

18.18 Review of User Access Rights must include the below:

1. Supplier must implement a documented process to review, verify and delete unnecessary user entitlements to Controlled Information Systems used to store, process, manage, and / or transmit Citi Information.
2. Supplier must review all user entitlements at least semi-annually and remove any unnecessary access.
3. Users must not review or approve their own entitlements or the entitlements of an individual who delegated review responsibility to them.
4. Following a function change by a supplier employee within Citi, the supplier has 14 calendar days to perform an access and entitlement review, and remove access to Citi data if no longer required for their new function.

18.19 Secure Log-on Procedures.

1. Login IDs associated with a static password must be locked out after a maximum of six (6) consecutive 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.

18.20 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. Passwords must contain a minimum of ten (10) characters, which must contain both letters and numbers, and be case sensitive.
4. 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).
5. All static passwords must be changed every 90 calendar days at a minimum.
6. All static passwords must be locked out after no more than six (6) consecutive failed login attempts. Passwords must be unlocked through an ID administrator function or automatically unlocked after at least 30 minutes.
7. All authentication systems must enforce a login inactivity/non-use control that cannot exceed 100 calendar days. If technically feasible, disabled logins may be re-enabled by the user or another authorized function.
8. The authentication process must ensure that the same password is not used within at least the last six (6) changes.

18.21 Use of System Utilities.

Supplier must ensure that the use of utility programs that can override system and application controls (e.g., booting up from peripheral devices) are restricted and controlled.

18.22 Session Time – Out

1. Login and re-authentication 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.
18.23 Termination of User Access.

1. Upon termination or resignation, user access or entitlements that could allow access to Citi Confidential or higher data including user login to Desktop/Active Directory, Single Sign-on (SSO), email, One Time Password (OTP) tokens and remote access must be removed immediately, or no later than the end of the next business day.

2. If an employee has access to Citi owned and administered systems, Citi Business Relationship Manager, BAO, or BAO support must be notified immediately upon function change or termination of that employee to ensure that the Citi Business Manager initiates removal of access for terminated workers by the end of their termination date.

3. Supplier has a documented process in place to retrieve the access from all assets in line with the timeframes set out in section ii when an employee or non-employee is terminated or resigns.

4. If any anomaly is discovered by the suppliers in regard to items i-iv, supplier must inform Citi Business Relationship Manager, BAO, or BAO support immediately, with a sound rationale and controls provisioned.

18.24 Remote Access.

The supplier must have remote access controls in place to protect access to networks that can store, process, or transmit Citi Confidential or higher data that include:

1. Remote access to Information Systems used to store, process, manage, and / or transmit Citi Information must be protected from unauthorized use.

2. All Supplier-managed laptops and all supplier-managed 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 higher, must be encrypted using an encryption tool that meets industry standards.

3. Remote connections must only be established through approved remote access solutions that employ multi-factor authentication (MFA).

4. 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.

5. Supplier managed devices must be regularly connected to the supplier network to receive and install regular updates of software / antivirus as a requirement for full access to the network. Limited access may be allowed for the express purpose of updating the device.

6. If non-company owned and managed devices are in use to access Citi Confidential or higher information, they must use an authorized solution that does not allow downloading to the local machine. The following controls must be in place:
   a) Citi Data is prevented from being downloaded to the personal device outside of a company-managed solution.
   b) The Supplier must ensure that such access is secured by either token-based or certificate-based authentication using standard remote access technologies (i.e., VPN, Virtual Desktop Interface (VDI), etc.).
c) Remote access solutions, such as Terminal Services and VMware Horizon must be configured to disable clipboard sharing and Drive Mapping over Blast, PCoIP, and RDP protocols

1. If soft tokens are used for MFA, such as a software application on a mobile device, the soft token authentication software must authenticate the user (e.g., by password, biometric, etc.) and prevent its use if the mobile phone is jailbroken or rooted (using an operating system other than those certified and supplied by the mobile device vendor).

2. All Supplier’s Personnel including, but not limited to permanent/temporary employees, contractors, and sub-contractors, requiring special, privileged, and/or administrative level access to systems, data repositories, applications and/or infrastructure, including, but not limited to, system administrators, database administrators, access control administrators, firewall administrators, web site administrators, etc., that are related directly or indirectly to Services provided for Citi must use multi-factor authentication and such access will be independently logged and monitored by Supplier for suspicious activity and/or or unauthorized access in accordance with Citi’s Requirements for Suppliers as hereinbefore noted.

3. All Supplier remote access personnel must attest and agree via documented evidence to the following:
   a) Will maintain a private, dedicated remote workspace that does not contain any voice assistance devices (e.g., Siri, Alexa), video recording devices, and/or any other photo, video, or audio listening/recording devices. No unauthorized personnel will be permitted to view any data, systems, applications that may appear on the remote computing systems’ screen(s).
   b) Will lock the computing device when leaving the device unattended to ensure that unauthorized access to view the screen is adequately mitigated.

18.25 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 conduct regular reviews of clear desks and clear screens to ensure protection of internal and confidential data is practiced at each company location. In addition, Suppliers are required to communicate this requirement to all its staff at least annually through IS awareness training.

18.26 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 semi-annually and tested annually.
18.27 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.

18.28 Operational Security Procedures and Responsibility.

1. Supplier must have a documented Change Management process.
2. Supplier must have a documented Capacity Management process that meets relevant industry standards.
3. Where applicable, Supplier must ensure that the Development, Test and Production environments are all physically and/or logically separated from one another.


1. Supplier must have documented and approved Software Development Lifecycle (SDLC) process.
2. Security Design Review must be included in SDLC with preventive and detective controls aligning with industry standards as OWASP.
3. Secure coding practices must be enforced.
4. Any critical vulnerabilities identified through intelligence gathering, vulnerability scans, or penetration testing must be prioritized and remediated within a well-defined timeframe commensurate with the vulnerability

18.30 Controls Against Malware.

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, ransomware, or other similar cyber-attacks in which data may be compromised) and must implement preventive, detective, and recovery controls to protect against such threats. Supplier must:

1. Implement, update, and maintain technology for anti-virus and anti-spyware on all personal computers and technology on all Local Area
Network (LAN) servers, mail servers and other devices that store, process and / or transmit Citi Information.

2. Have security settings in place to prevent end users from disabling the anti-virus/antimalware and scheduled scans.

3. Have centrally managed, automated procedures for configuring and updating antivirus and anti-malware software.

4. Ensure processes are implemented for identifying and addressing non-compliant computers where the anti-virus signatures or scan engines are outdated.

5. Control access to communication ports / interfaces that allow connection to external devices including but limited to storage media.

18.31 Controls Against Mobile Code.

Suppliers must ensure that necessary precautions are taken to control the use of Mobile Code. When Mobile Code usage is authorized, the configuration must, at a minimum, meet all relevant 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.

18.32 Audit Logging.

Supplier must ensure that all Controlled Information Systems used to access, store, process, manage 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.

2. All system alarms associated with a firewall or IDS / IPS generated security event.

3. All attempted violations of system security (e.g., failed User login attempts).

4. All significant events relating to financial transactions and Citi Information which specifically include the following items:

5. Updates to financial transactions

6. Updates to Confidential PII data

7. Updates to Restricted data

8. Updates to Authentication data

9. Session artifacts, such as unique device ID must be captured, when technically feasible, and logged for Citi-facing applications (i.e., websites and mobile applications) to support fraud investigations. These artifacts
must at minimum contain IP addresses. These artifacts must be captured for Citi transactions and for Citi account opening activity. Information must be captured so the session artifact can be linked to the transaction or account opening.

10. Significant Information Security Administration (ISA) events must be logged specifically including the following items:
   a) User creation
   b) Modification of user access rights
   c) Deletion, creation, and modification of profiles on Controlled Information System
   d) Password reset
   e) Changes to system security configuration
   f) All interactive activity of privileged Functional IDs must be logged
   g) 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.)

18.33 Protection of Log Information.

Supplier must ensure that access controls are present to preserve the integrity of audit trails during initiation, shutdown, while in storage, and transmission.

1. 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.
2. Supplier must define, maintain, and comply with a record retention procedure for log data that complies with the Citi Records Management Policy and all applicable legal and regulatory requirements.
3. The clocks of all relevant information-processing systems within an organization or security domain must be synchronized with an accurate time source.

18.34 Monitoring System Use.

The following events must be captured, logged, and reviewed directly or through an automated review process:

1. All system alarms associated with a firewall or Intrusion Detection Systems (IDS) / Intrusion Prevention System (IPS) generated security event.
2. All updates to critical resources as identified in the secure standard build.
3. All interactive activity performed by privileged or CDA functional IDs or temporary ID.
4. Significant ISA Events listed in the Audit logging section above with the following Exception:
   a) Removal of entitlements from user, role, or profile where Information Security Administration activity is executed by an automated workflow / fulfillment system that has end-to-end integrity controls.

18.35 Log Correlation and Review.

1. When a logged event triggers an alert, the event is reviewed, follow up actions and investigation must be pursued if it indicates a potentially harmful information security incident may have occurred.
2. Supplier must ensure audit logs are aggregated to a central log management system like a Security Information and Event Management (SIEM) or log analytic tool for log correlation analysis and review. This may be a feature of their central log management system or may be a separate tool. Low risk vendors are exempt from this requirement.
3. High-risk suppliers must periodically review and adjust the configuration of their SIEM or log analytic tool to improve the identification of actionable events.

18.36 Control of Operational Software.

Supplier must ensure that 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.

Supplier must ensure that a documented process is implemented that specifies the time periods within which all approved security patches and configurations are applied.

Regardless of any separate maintenance agreement between Supplier and Citi, Supplier must ensure that software developed for Citi and governed under a license agreement does not require use of versions of non-supported software with known vulnerabilities, and updated, and patched as required, in a timely manner.

Open-source application software used to process Citi Information must be acquired from established suppliers and must be licensed, catalogued and supported.

18.37 Vulnerability and Threat Management.

If the Supplier maintains or stores Citi Confidential Information on a website or Internet accessible system, or a website that is Citi branded, then, to protect against a vulnerability or threat that involves products or services affecting Citi (each a “Vulnerability”), the Supplier must comply with the following Requirements:

1. Appoint one Supplier employee, knowledgeable about information security matters, to respond to Citi’s inquiries regarding information security.
2. Use commercially reasonable efforts to monitor, on a regular basis, reputable sources of computer security vulnerability information, such as FIRST,
CERT/CC, CISA Known Exploited Vulnerabilities Catalog, and vendor mailing lists, and take appropriate measures to obtain, thoroughly test, apply, and provide to Citi relevant service packs, patches, upgrades, and workarounds.

3. Test, on at least a quarterly basis, the implementation of its information security measures using network, system, and application vulnerability scanning tools and/or penetration testing.

4. Permit Citi to perform at reasonable times, Vulnerability, ethical hacks, or other security assessments, to verify Supplier compliance with its obligations under any Contract and these Requirements, including but not limited to, review of policies, processes, and procedures, on-site assessment of physical security arrangements, network, system, and application vulnerability scanning, and penetration testing, using commercially available tools and/or industry standard practices to perform these inspections.

5. Maintain, for a period of at least 180 calendar days (or such longer period as may be required by law or contract) detailed log files concerning all activity on Supplier’s systems including, without limitation:
   a) All sessions established
   b) Information related to the reception of specific information from a user or another system
   c) Failed user authentication attempts
   d) Unauthorized attempts to access resources (software, data, processes, etc.)
   e) Administrator actions
   f) Events generated (e.g., commands issued) to make changes in security profiles, permission levels, application security configurations, and/or system resources.

5. All log files must be protected against unauthorized access, modification, or deletion. In addition, the Supplier must maintain records related to privacy or other security information risk assessments as well as records related to routine security actions and investigations, if and as applicable, in accordance with Citi’s Records Management Policy, including Citi’s required retention period for such records.

6. Where Supplier utilizes contractors or subcontractors to provide the Services, Supplier must, at its own expense, ensure that any Vulnerability assessments required under these Requirements herein are completed in the same timely manner as if Supplier were providing those Services directly and shall ensure that the requirement for any contractor or subcontractor to facilitate any such assessments must be memorialized in the agreement between Supplier and contractor/subcontractor pertaining to the Service, including language authorizing Citi to perform such assessments.

7. If Supplier is acquired or acquires another entity in any merger or acquisition or similar transaction, and such transaction may impact the Services, Supplier must promptly notify Citi in writing and
Supplier must perform an information security assessment on the resulting entity consistent with these Requirements to ensure such change does not impact compliance with the same.

8. **Process Implementation.** Supplier must implement a vulnerability and threat management process that comprehensively addresses and/or includes all the following:
   a) Discovery and management of Vulnerabilities in all assets that can be used to process, store, access or transmit Citi Confidential or higher data
   b) A requirement that at least monthly scans using a tool that discovers instances of the occurrence of currently known Vulnerabilities is conducted
   c) Ranking of Vulnerabilities in accordance with the “Common Vulnerability Scoring System (CVSS) v3.1” (see https://www.first.org/cvss), with remediation timelines based on the severity
   d) A requirement for testing Vulnerability fixes prior to full production deployment
   e) An emergency process for remediating critical Vulnerabilities
   f) If the supplier hosts Citi Confidential or higher data on Internet-based applications and infrastructure, there must be an annual Vulnerability Assessment "Penetration Test" completed by the supplier or an external party that specializes in these types of assessments
   g) The supplier must track assets that are approaching or have reached a status of End of Life (EOL) or End of Vendor Support (EOVS) status and has processes in place to upgrade or replace such assets.
   h) Any critical vulnerabilities identified through intelligence gathering, vulnerability scans, or penetration testing must be prioritized and remediated within a well-defined timeframe commensurate with the vulnerability risk

9. **Notification.**
   a) Where Supplier identifies a Vulnerability that involves a product or service affecting Citi, Supplier must notify Citi in writing within 48 hours of identification and include a description of remedial actions being taken by Supplier.
   b) Where Supplier becomes aware of a Vulnerability that involves a product or service affecting Citi following responsible public disclosure of process channels (publication of Vulnerability in National Vulnerability Database (NVD) or via threat catalogue provided to external security vendors), Supplier must notify Citi in writing within 48 hours of such publication. Each notification must include information about the Vulnerability, if the Vulnerability impacts Citi, if it can be exploited remotely; and the Common Vulnerabilities and Exposures (CVE) score. Supplier must continue
to provide updates to Citi until the Vulnerability is remediated. In cases where Citi identifies a Vulnerability, Citi may provide notice to Supplier of the same, and Supplier shall promptly remediate the Vulnerability in accordance with this Section.

10. Remediation.
Following the notification requirements outlined in section x, the supplier must complete the following for remediation of the vulnerability:
   a) Once a risk level is assigned and agreed, Supplier must remediate any identified medium, high, or critical Vulnerability.
   b) Where possible, the fix to any impacting Vulnerability must be made available in a security package against the currently deployed release.
   c) If Supplier is unable or unwilling to remediate the Vulnerability to Citi's satisfaction within the designated timeframe, then Citi may terminate the applicable license without any further liability or financial obligation (for the portion terminated) and Supplier shall promptly refund to Citi the pro-rated portion of the license fees paid.

18.38 Communication Security Network Controls
1. Supplier networks used to access, store, manage, process and/or transmit Citi Information must be protected from threats and security must be maintained for the Information Systems using 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).
   a. Networks used to access, store, manage, process and/or transmit Citi Information 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.
   b. All external IP connections to the Supplier global network are protected by a Supplier managed firewall.
   c. 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 accessed, managed, stored, processed, or transmitted.
3. All Citi branded Internet applications and, Supplier must ensure that:
   a) Services hosted at Supplier sites must have Citi approved anti-DDoS (Distributed Denial of Service) services or comparable controls validated by Citi.
   b) External firewalls must be configured with a default “deny all” rule. Firewall rules must be configured based on the least privilege principle and all connection attempts that are denied by the firewall (e.g., drop packets) shall be logged/recorded.
c) Deny network communications traffic is the default and allow network communications traffic is by exception at managed interfaces. The exceptions must be very limited to specific source, destination, and service.

18.39 Segregation in Networks.
Supplier must ensure that all Information Systems and applications used to access, store, process, manage and / or transmit Citi Information and are accessible via the Internet, are only accessed via the Supplier’s demilitarized zone (DMZ).

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).

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 may be done at the group or individual level.

18.40 Equipment Identification in Networks.
Technology platforms must identify and authenticate peer technology platforms commensurate with the IS Risk Levels of the interaction and other mitigating controls.

1. Only Supplier devices (i.e., hardware, including, but not limited to, desktops, laptops) that comply with these requirements 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 requirements and authorized by Citi may have access to the Citi network.

Supplier must incorporate information security procedures in its processes and procedures for the selection, development, and implementation of applications, products, and services.
18.42 Online Transactions.

1. Where applicable, Supplier must have Information Systems that use dynamic passwords or digital certificates to validate the credentials.
2. All end-entity certificates must be replaced at least once every two (2) 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 that store, process, manage or access Citi information, host Citi branded Internet facing applications, or have connectivity to Citi’s network resources must:
   a) Possess an authentication method based on the types of data / functions accessed;
   b) Perform a Multifactor Authentication (MFA) compliance assessment;
   c) Implement an online Suspicious Activity Management (SAM) solution
   d) In all these cases, Supplier should contact its primary business contact for the current requirements.

18.43 Change Control Procedures

1. Supplier must ensure that configuration changes to firewalls, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are routed 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 “Availability” of “High”, logs captured according to Section 18.35 (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 changes that are part of the temporary privileged access were made as intended.
5. The supplier must document all changes, including storing evidence of the review process.

18.44 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.

18.45 Test Data.

Confidential or higher risk information as defined by Citi must not be used or stored by Supplier in software application(s) development or testing environments unless that information is de-identified, masked, and/or obfuscated using tools and methods that meet
industry standards, so that such data is no longer sensitive, or implement live production controls within the development or testing environments.

18.46 Transmission of Data.
Supplier must not transmit Confidential or higher classification information over any public network (such as the Internet) in an unencrypted manner. Should Confidential or higher classification information as defined by Citi be sent over public networks, that information must be encrypted using an encryption algorithm, strength, data recovery, and key stores that are consistent with Citi’s policies and standards (e.g., refer to Section 18.9 – 18.12) and/or mutually agreed current industry standard encryption protocols.

18.47 Off-Network Data Storage.
Supplier shall, when storing Citi’s Confidential or higher risk information outside of Supplier’s network (e.g., Disaster Recovery backups), ensure that such information is encrypted when at rest using a Citi approved encryption algorithm (e.g., refer to Section 18.9 – 18.12) and/or mutually agreed current industry standard encryption protocol and strength, and key store.

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

18.49 Reporting Information Security Weakness.
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.

18.50 Security Incident 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 Citi customers or the franchise (including where the incident involves a significant number of customers; a large dollar amount; likely to be the subject of press coverage; or likely to result in the non-routine notification of a regulator) must be reported within 2 hours and all other security incidents must be reported within one business day 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).
18.51 Reporting Security Incidents.

1. Suppliers are required to report any Security Incident that compromises or endangers the confidentiality, integrity, or availability of Confidential or higher Citi owned or managed 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 security incident occurred. This includes, but is not limited to, the alteration, destruction, disclosure, loss, theft, or misuse of said data or systems, devices, or physical or electronic media containing this data. This could also include public facing assets of any data classification, as well as any Personally Identifiable Information (PII) / (Personal Data) data breach where it is likely to result in a high risk to the rights and freedoms of natural persons, where such rights and freedoms are defined by local laws or regulations.

2. Third party vendors are required to report actual or potential security incidents to their management, who must immediately notify an officer of Citi in the event of any actual or likely disclosure of Citi Confidential or higher information. The Citi representative must notify their ISO immediately.

18.52 Data Leakage Protection (DLP).

1. Supplier must implement data leakage prevention (DLP) controls, including content and endpoint monitoring that covers all staff with access to Citi Confidential or higher data.

2. The supplier must have controls in place to detect and/or prevent instances of Citi Confidential or higher data being moved off their network via the following channels:
   a) Unencrypted emails.
   b) Encrypted email attachments.
   c) Uploading Citi data to external web sites, especially SaaS/file sharing sites.
   d) Printing of Citi data.
   e) Transfers of Citi data to locations outside of their network (for example via FTP).
   f) Attempts to copy Citi Confidential or higher data to removable media such as USB drives, removable hard drives, CD/DVD drives, and other removable devices with data storage capabilities.
   g) The DLP solution must log and alert the supplier of all events that represent attempts (whether successful or blocked) to move, transport, or copy Citi Confidential or higher data from their network to other destinations.
18.53 Web Browsing.

1. Supplier must have web-access controls in place to prevent the sharing of Citi Confidential or higher information and exposure to malware or attack for those employees with access to Citi data.

2. For suppliers who have access to Citi Confidential or higher data:
   a) All URL requests must be logged.
   b) Attempts to access sites that can be used for unauthorized sharing of Citi data (i.e., webmail, chat, social media, online storage, etc.) must be blocked.
   c) Access to sites that can expose the environment to malware or attack must be blocked.
   d) Attempts to access sites that are deemed non-business related must be blocked.
   e) The supplier must subscribe to a URL categorization service that is regularly updated; all URLs not categorized are blocked by default or all URLs are blocked by default and URLs are approved on a case-by-case basis. Low risk suppliers are exempt from this requirement.
   f) Web Browsers that are in use by the supplier are fully supported and up to date with the latest security updates by the software vendor.

18.54 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 18.9 (Policy on the use of cryptographic controls).

18.55 Email.

The supplier must have e-mail controls in place to prevent the sharing of Citi Information and exposure to malware or attack. This includes:

1. Incoming file attachments entering the e-mail gateway are scanned and blocked if they pose a risk to the system.
2. E-mail filtering (Anti-Spam, Anti-Phishing) software is in use and is up to date.
3. Any Citi Confidential or higher data must be encrypted when sent outside of the organization.
4. E-mail Clients that are in use by the supplier fully supported and up to date with the latest security updates provided by the software vendor.

18.56 Removable Media.

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.

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.

If the use of removable media is allowed, such usage must have a management approval process, including the business rationale requiring the use of removable media.

Removable media must be inventoried by Citi Management.

Removable media that contains Citi Confidential or higher data must be automatically encrypted with no action required by the user.

18.57 Media Disposal.
1. 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.
2. An approved tool that randomly overwrites the drive sectors with specific, different characters must be used to securely erase mountable media based on the following rules:
   a. For media that stored information classified as Confidential or higher the tool must complete three passes of the media.
   b. Degauss the media (if applicable).
3. Destroy the media physically to make it unreadable (i.e., shredding, crushing the drives).
4. Paper and other non-electronic storage media containing Confidential or higher Information must be securely collected and stored in a secure “Confidential Bin” before final disposal. Confidential Bins must always be locked and can only be opened by authorized personnel.
   a) Copiers, Printers, Fax Machines, and any other device that has memory/storage that may contain Citi Confidential or higher information must be sanitized as well.

1. The supplier must ensure all employees, including contractors and temporary staff receive appropriate awareness education and training on organizational policies and procedures as relevant to their job function.
2. They must ensure that the training and awareness program is reviewed and updated annually.
3. At a minimum, the following topics must be included:
   a) Acceptable use of assets
   b) Information labeling and handling
c) Secure Transmission (Secure Email, Secure SharePoint Storage, not sending Citi owned data to personal email)

d) Information security incidents reporting

e) Secure Workplace (Appropriate Internet Usage, Unauthorized Software, not downloading non-Citi approved software)

f) Password Management (Strong Passwords, Password Sharing)

g) Malware Controls

h) Social Engineering (Phishing, Spear Fishing, Vishing SMiShing)

i) Remote Working (Secure/Safe Connection, Personal Device Security)

4. Supplier must ensure that all employees, including contractors and temporary staff complete the information security awareness trainings within 30 days of hire.

5. Supplier must ensure all employees including contractors and temporary staff complete annual refresher training.

6. Training should include a measure of its effectiveness.

18.59 Cyber Risk Management Program.

Supplier must also, at a minimum, maintain an appropriate cyber risk management program that includes the following:

1. Maintain a well-defined, documented, and Information Security Risk Management program, and/or an operational risk management program that has a clearly defined cyber/information risk management component, that defines the Supplier’s cyber risk appetite and ensures that its cyber-residual risk aligns with that appetite.

2. Robust security risk management governance program that includes, but is not limited to, the collection of and/or the performance of security audits and reviews that assess the overall state of security within the organization, and routinely report at least annually to its executive leadership for review and assurance that the supplier’s cyber risk appetite has not be breached

3. Maintains compliance with PCI Data Security Standards (PCI-DSS) applicable to Supplier where Supplier is processing, storing, and/or transmitting credit/debit card transactions, payments, and/or information.

4. Maintains a crisis management plan and playbook Security incident Response Team (SIRT) plan consistent with industry standards to ensure Supplier has sufficient and adequate capability to detect, contain, investigate, respond, and recover from any attempted, suspected, and/or actual cyber security incident including, but not limited to ransomware, unauthorized access, unauthorized data exfiltration, application source code theft, etc.
5. Maintain an effective cyber hygiene program that ensures software patches are installed and configurations of networks, systems and/or applications are applied and maintained in a consistent, secure manner.

6. Maintain an appropriate cyber/information security and privacy awareness and education program that includes, but is not limited to, preventing phishing and other social engineering attacks, appropriately handling of confidential and/or privacy regulated information, and security incident reporting and response management.

18.60 Application, API, Code, System, and Infrastructure Security.

Where Supplier is hosting, developing, co-developing, providing development environments, and/or supplying a software application(s), Supplier shall perform code reviews of said software and/or patches to the software for security flaws, prevention of unauthorized access, modification, and/or insertion of malware or other forms of malicious code, and vulnerability testing to ensure that the application (including APIs), along with underlying system services, operating system, and that networks are free of known vulnerabilities and defects that could result in a security incident, privacy breach, fraud, unauthorized access and/or disclosure of Confidential Information, loss of integrity of the information being processed, stored or transmitted by the application(s), and/or loss of availability that could affect the quality of products and/or services that supplier provides Citi.

19. SECURE WORKPLACE GUIDELINES

Applicable to Suppliers that access/process/manage/store Citi Information AND/OR Host Citi branded internet-facing applications AND/OR have connectivity to Citi’s network resources AND/OR require unescorted access to Citi facilities.

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 Suppliers. 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.

<table>
<thead>
<tr>
<th>Item</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citi Information (electronic and hard copy documentation)</td>
<td>Lock up and secure Citi Information after normal work hours and anytime Supplier is away from designated workspace.</td>
</tr>
<tr>
<td>Item</td>
<td>Requirements</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Desktop Personal Computers (PCs) and Laptops</td>
<td>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 &quot;Lock Computer&quot;. 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.</td>
</tr>
<tr>
<td>Lock It Up</td>
<td>File cabinets and drawers that store Citi Information must be locked after normal work hours.</td>
</tr>
<tr>
<td>Open Office Areas</td>
<td>Open office areas must not be used as file server / mini data centers to store Citi Information unless specifically designed for such use and documented with Citi.</td>
</tr>
<tr>
<td>Printers, Photocopiers and Fax trays</td>
<td>All Citi related material must be cleared from printers, photocopiers and fax trays.</td>
</tr>
<tr>
<td>Disposal</td>
<td>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.</td>
</tr>
</tbody>
</table>

**20. ARTIFICIAL INTELLIGENCE/MACHINE LEARNING**

*Applicable to Suppliers that utilize Artificial Intelligence/ Machine Learning (AI/ML), as defined by Citi in these Requirements for Suppliers, in any part of the product/service that they are providing.*

Supplier shall deliver written notification to Citi that expressly identifies AI/ML, as defined by Citi in the Appendix hereto, where such AI/ML is:

1. Used, contained, or otherwise incorporated in any product or service for which they are under Contract to directly or indirectly provide to Citi, or in any part thereof, including any third-party product or service contained or embedded therein; or
2. Utilized in any manner in Supplier’s performance of any Contract, whether or not such AI/ML is used, contained, or otherwise incorporated in the actual product or service being delivered to Citi; or
3. Utilized by Supplier in any manner which may expose Citi Information to such AI/ML, including, but not limited to, any AI/ML utilized by Supplier in its non-commercial business operations (e.g., business record keeping, process improvements, research and development, compliance, and internal audit).

**20.1.** Supplier shall ensure that any agreement governing its relationship with a subcontractor (or that subcontractor’s own agreement with another relevant party) engaged to perform, or assist with, Supplier’s obligations under any Contract, or
any agreement between Supplier and a third party governing such third party’s provision of services in support of any Supplier non-commercial business operation referred to above, contains provisions that are, at a minimum, as comprehensive and strict as those contained in this Section 20, and Supplier shall exercise its rights under such provisions for Citi’s benefit at Citi’s request. Additionally, throughout the life of the Contract, any utilization of AI/ML as described in this Section 20 at any stage must be promptly notified to Citi in writing, and Supplier shall promptly comply with any Citi request for further supporting information relating to such AI/ML and its utilization, and may be subject to additional review, changes, and oversight of such AI/ML, where appropriate.

20.2. If requested by a regulator, as part of any regulatory inspection or forensic investigation into the use of AI/ML in any part of the product/service, the Supplier must assist Citi in responding to the regulator’s request, including conducting and/or facilitating the conduct of algorithm audits necessary to discover the actual operations of algorithms comprised the AI/ML models.

20.3. The following principles must also be adhered to:

1. Legality. Supplier AI/ML systems is expected to be designed to adhere and comply with applicable law and to international treaties that are most protective to Citi’s customers, users, and employees.
2. Purpose and Proportionality. Our AI/ML systems will be designed for the fulfillment of the intended purposes of the services provided to Citi, and will solely operate proportionally to the extent necessary, adequate, and relevant in relation to the aforementioned purposes.
APPENDIX - DEFINITIONS

Air – Gap is a security measure in which a computer, system, or network is physically separated from other computers, systems, or networks. An air-gapped data backup architecture limits exposure to a cyber-attack and allows for restoration of data to a point in time before the attack began.

Applicable Law includes: (a) state foreclosure laws and regulations and (b) the rules, guidelines and other releases issued by various United States Federal Agencies, including the Office of the Comptroller of the Currency (sometimes referred to as Red Flag Guidelines and Regulations) implementing section 114 of the Fair and Accurate Credit Transactions Act of 2003.

Availability Zone is where the Cloud Service Provider has a group of logical data centers. An Availability Zone is one or more discrete data center(s) with redundant power, networking, and telecommunications in a Cloud Region.

Artificial Intelligence (AI) refers to a quantitative method, system or approach (‘techniques’) that emulates human intelligence via computer programs to make estimates, predictions, recommendations or decisions in manners that go beyond classical statistical, mathematical, econometric or financial approaches. AI Categories include:

- Static AI: AI techniques manually trained offline or whose parameters are explicitly programmed and then used to make estimates, predictions, recommendations, or decisions.
- Dynamic AI: Techniques that, unlike “Static AI”, can automatically retrain parameters periodically, in production.
- Auto AI: “Dynamic AI” techniques that additionally are capable of automatically changing their basic structure (e.g., hyperparameters, input variables).
- Cognitive AI: Techniques that can autonomously make decisions and take actions accordingly, even on matters for which they were not specifically trained.

Machine Learning (ML) is the subset of AI that derives representations or inferences from data without explicitly programming every parameter representation or computer step, for example Random Forests, Neural Network-based approaches. In contrast, AI techniques that are not members of the ML subset include techniques such as fuzzy logic, complex dependency parsing techniques for natural language processing.

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 Information is information which Citi owns or is obligated to protect during storage, processing, transmission, or disposal in both digital and non-digital formats. Citi Information Classifications Include:

- 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 Personal Identifiable Information (CPII)** 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, or 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 that when combined with other information constitute Confidential PII:
  o Individual name or contact information (address, telephone, or email address) in combination with:
  o Passport number, driver’s license number, national or government ID number, or an individual’s tax ID number;
  o Customer Identification number, Credit/Debit card number, Account identifiers that may result in funds movements, or other financial account number;
  o Transactional data elements that can be used for identity theft or fraud;
  o Customer account application information, credit report data, credit score;
  o Worker performance appraisal or compensation information;
  o Video recordings including CCTV and ATM records
  o These elements are considered Confidential PII, either alone or in combination with other elements: 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.

• **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.

• **Personal Identifiable Information (PII)** Personal Information is any information that:
  o identifies or can be used to identify an individual or household (such as name, signature, address, unique national identifier such as social security number resident registration number, date of birth, driver’s license number).
  o relates to, describes, is capable of being associated with, or could reasonably be linked (directly or indirectly) with an individual or household;
  o can be used to authenticate an individual or provide access to an account (such as username, email address, password, PIN, identification number, answers security questions); or relates to an individual and that might be sensitive (such as personal medical or health information, account number, account value).
  o Personal Information also includes Protected Health Information (as defined by the U.S. Health Insurance Portability and Accountability Act), Sensitive Personal Information and Credit Information (as defined in various data protection/privacy and bank confidentiality laws).

• **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.

• **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.

• **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). 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.

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.

Cloud Region is a physical location where the Cloud Service Provider clusters data center(s).

Communications Equipment, Systems and Services are any hardware, software or applications used in the transmission of written, voice, or video electronic communications. eComm Channels include but are not limited to: computers, laptops, tablets, mobile devices or mobile phones, including “Bring Your Own Device” (BYOD), BlackBerry, telephone, facsimile (fax services), intranet and internet access, Wi-Fi Services, e-mail services, instant messaging services such as Microsoft Lync, Skype, and Bloomberg messages, websites and applications with embedded communications features, video meeting or collaboration platforms such as Zoom or Microsoft Teams, and social media services, interactive information sharing services, third party chat rooms, electronic bulletin boards and blogs.

Content means Citi’s Confidential Information and any other data, reports, statistics or information of any kind (a) furnished or made available directly or indirectly to Supplier by or on behalf of Citi or its Affiliates or by or on behalf of its or their clients, customers or service providers, (b) created, produced via the Services, or (c) derived from any of the foregoing.

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.

Denial of Access (DOA) Test validates the staffing and support for Citi business processes that can be recovered within the defined RTO.

Denial of Service (DOS) Test is 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.

Electronic Communications are messages or information sent, received, or used by Personnel using electronic means, carried over wire or by wireless signals. Electronic Communications include but are not limited to text messages, email, peer-to-peer or instant messages, blog posts, social media posts, messages sent through messaging applications such as WhatsApp, WeChat, Line, Signal, or Viber, and include attachments, screenshots, recorded voice or video files, live voice or video, and files created, received, downloaded, stored, transmitted, deleted or used via Electronic Communications Equipment, Systems, and Services.
Functional IDs are a generic ID, such as ADMIN or ROOT, which 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.

Franchise Critical Processes / Franchise Critical Applications (FCA) are those processes / applications that have been identified by Citi as essential to the successful execution of its Franchise Critical Business Functions.

Fraud is an intentional act, misstatement or omission designed to deceive others, resulting either in the victim suffering a loss or the perpetrator achieving a gain.

Hosted Services include any Installed Applications, and any facilities and environment managed or utilized by Supplier to provide the Hosted Services, all applications and other software, databases, websites, servers, hardware, networks, telecommunications and other equipment, and other technology installed or used within the Hosted Services environment, and, in each case, all Updates and Support Services, but excluding all Content and Citi’s Systems.

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.

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.

Non-Client / Non-Revenue Generating is defined as business critical activities not associated with revenue generating activities including legal, supervisory, regulatory and Continuity of Business activities.

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.

Personnel: means, whether stated directly or derived from context, Supplier and its affiliates, directors, officers, employees, agents, auditors, consultants, service providers, and contractors (excluding Citi personnel). Supplier personnel also include the directors, officers, employees, agents, auditors, consultants, or other representatives of any Subcontractor."

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.

Recovery Capacity is 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.

Recovery Duration is the maximum duration, in calendar days that the Supplier is capable of sustaining operations whilst in recovery mode.
Recovery Point Objective is 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.

Recovery Time Objective is the duration in hours between the time of a service disruption and the restoration of products and services.

Resource Management Organization (RMO) is responsible for the global end-to-end resource management for Citi, including Strategic Sourcing, Purchase to Pay Operations, Staffing Office, and Supplier Management Framework.

RMO Sourcing Manager is an individual within Resource Management Organization (RMO) 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.

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.

Subcontractor: A subcontractor is a fourth party (person or entity), who was hired by a third party to perform some or all of the services or activities that Citi has contracted to the third party.

Guidance:

Q1: Do all of the Third Party's subcontractors need to be reported?

A1: Only subcontractors related to the service being performed need to be reported. Examples of services or activities performed by a subcontractor include, but are not limited to:

* A subcontractor performing technology or software services that directly or indirectly support the service/activities that Citi has contracted to the Third Party; or

* A subcontractor whose services include access to Citi Confidential or higher information; or

* A subcontractor who has direct or indirect interaction with any existing/potential Citi Client; or

* A subcontractor who is unescorted and performs shredding or archiving services of Citi documents within or outside of any Citi premise; or

* A subcontractor supporting core banking functions or services such as payments, collection, lending, etc.

Technology Recovery Time Capability (TRTC) is the estimated total restoration time for an application/business service and its underlying infrastructure components to be recovered at its disaster recovery or alternate site following an invocation.