CITI REQUIREMENTS FOR SUPPLIERS
(Formerly Known as CITI Standards for Suppliers)

SECTION 2
(Applicability based on criteria specified for each topic)

OWNER:
GLOBAL HEAD OF RESOURCE MANAGEMENT ORGANIZATION (RMO)

ISSUE DATE:
JANUARY 2015

REVISED:
FEBRUARY 2021

VERSION:
5.0
TABLE OF CONTENTS

1 GENERAL OVERVIEW.................................................................3
2 RECORDS MANAGEMENT..........................................................4
3 GLOBAL COMPLAINTS / CONCERNS MANAGEMENT STANDARDS .....5
4 CONTINUITY OF BUSINESS.........................................................6
5 GLOBAL BACKGROUND SCREENING STANDARDS .......................9
6 EXPENSES..................................................................................11
7 INFORMATION SECURITY (IS).......................................................12
8 SECURE WORKPLACE GUIDELINES.............................................31
1 GENERAL OVERVIEW

1.1 PURPOSE

The purpose of the Citi Requirements for Suppliers (“Requirements”) Section II is to facilitate Suppliers’ compliance with Citi policy requirements, based on the applicability criteria identified for each policy area.

Section II of the Requirements provide specifics on Citi’s policy requirements. Each Citi business and legal entity may also indicate additional requirements for Suppliers in the transactional document (work order or license). These requirements and limitations can be also reflected in business-specific policies, including any policies applicable to Suppliers. In the even such entity-specific policies differ from these Requirements; the more restrictive policy will prevail in order of interpretation. Suppliers must take a proactive role and consult with their primary Citi business contact (or his or her designee) regarding any questions they may have to ensure compliance with current Citi policies, or any changes as notified.

Please refer to the Citi Requirements for Suppliers Section I for general overview of policy requirements applicable to ALL Suppliers.

1.2 Applicability Criteria

<table>
<thead>
<tr>
<th>Section #</th>
<th>Section Title</th>
<th>Applicability</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>RECORDS MANAGEMENT</td>
<td>Suppliers with access/process/store Citi Information</td>
</tr>
<tr>
<td>3</td>
<td>GLOBAL COMPLAINTS / CONCERNS MANAGEMENT STANDARDS</td>
<td>Suppliers engaged in customer-facing activities on behalf of Citi</td>
</tr>
<tr>
<td>4</td>
<td>CONTINUITY OF BUSINESS</td>
<td>*Applicable if the product/service provided by the supplier is 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 (BAO) is responsible for communicating applicability and COB requirements to the Supplier</td>
</tr>
<tr>
<td>5</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 (Such personnel would be required to have a GEID, and be registered in Citi’s Non-Employee Management System)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*Applicable to suppliers that access/process/store/manage Citi Confidential or Higher Information</td>
</tr>
<tr>
<td>6</td>
<td>EXPENSES</td>
<td>Suppliers that are contractually eligible to claim reimbursable business expenses</td>
</tr>
<tr>
<td>7</td>
<td>INFORMATION SECURITY (IS)</td>
<td>Suppliers that access/process/manage/store Citi Information AND/OR Supplier responsible as a Host for Citi branded internet facing applications AND/OR Suppliers with connectivity to Citi’s network resources AND/OR</td>
</tr>
<tr>
<td>8</td>
<td>SECURE WORKPLACE GUIDELINES</td>
<td>Suppliers requiring unescorted access to Citi facilities</td>
</tr>
</tbody>
</table>
2 RECORDS MANAGEMENT

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

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

Suppliers must not dispose of any Citi Information, irrespective of its classification (e.g., Confidential, non-Confidential) without their primary Citi business contact or BAO approval, which must include confirmation that no active Record Holds apply to the Information due for disposal. 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 (RMO) to review and update contact names, procedural details, roles and responsibilities and the Supplier Record Inventory.
3 GLOBAL COMPLAINTS / CONCERNS MANAGEMENT STANDARDS

*Applicable to suppliers engaged in customer-facing activities on behalf of Citi

3.1 OVERVIEW

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

Citi’s consumer facing suppliers have different interaction models with consumers; therefore, Third Party Supplier Management may leverage the below approaches to comply:

➢ If the Supplier handles Complaints/Concerns themselves, they must comply with the requirements in the U.S. Consumer Complaints/Concerns Procedures.
➢ If the Supplier chooses to not handle Complaints/Concerns, then the Supplier must:
  • Deploy Citi’s definition of a Complaint/Concern (to ensure they know how to identify)
  • Implement procedures/practices to provide the Complaint/Concern to Citi for handling without placing unnecessary burden on the consumer to contact Citi.

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

3.2 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.
4  CONTINUITY OF BUSINESS

4.1  OVERVIEW

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

4.2  RECOVERY RESOURCES

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

4.3  RECOVERY SERVICE LEVELS

Supplier's business continuity must meet established levels of service in order to be effective for Citi. At minimum, Supplier's business continuity plan shall establish specific values for (1) Recovery Time Objective; (2) Recovery Point Objective; (3) Recovery Capacity; AND (4) Recovery Duration.

A supplier that hosts Citi Franchise Critical Applications (FCAs) used for critical transaction processing, must have an “air-gap” measure for backing up critical data required for recovery so that backup data is immutable and/or stored offline (disconnected from the network), and restoration of data can be achieved within the required Technology Recovery Time Capability (TRTC). (Refer appendix for definition of terms).

4.4  DISASTER RECOVERY PLAN

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

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

4.5  CRISIS NOTIFICATION

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

*Applicable if the product/service provided by the supplier is 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 (BAO) is responsible for communicating applicability and COB requirements to the Supplier.
4.6 TESTING

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

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

Suppliers must test the following disruption scenarios:

1. Denial of Access (DOA)
2. Denial of Service (DOS)

A. Citi Participation / Review of Supplier’s Testing

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

For Denial of Access (DOA) tests:

1. Most Critical Applications / Processes to 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:

1. Processes with an RTO <= 72 hours, Citi will participate in or observe Supplier’s testing activity for all applications. Supplier permits Citi to review recovery plans covering technology, test scripts, test results, and evidence.
2. Processes with an RTO > 72 hours, Unless otherwise requested by Citi, Citi will require Supplier’s attestation for recovery planning covering business and/or technology (as applicable), test scripts, and test results.

B. 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).

C. Volume Testing

A supplier that hosts Citi 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.

4.7 CRISIS MANAGEMENT

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

4.8 ASSESSMENTS

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

1. Suppliers supporting processes with an RTO <= 24 hours must be assessed on an annual basis
   - Assessments for suppliers supporting Franchise Critical processes must be conducted at the supplier’s site
2. 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

The assessment will consist of business recovery questionnaires requiring responses from Supplier with evidences. 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.
5 GLOBAL BACKGROUND SCREENING STANDARDS

5.1 OVERVIEW

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 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 here.

5.2 COLLECTION OF BASIC INFORMATION AND IDENTITY VERIFICATION

Prior to any Supplier’s personnel beginning a Citi assignment, Suppliers must collect the individuals’ first and last name, mailing address and permanent address (if different), telephone number and e-mail address (if applicable). Supplier’s Personnel must also provide documentation which validates their identity. This may include providing information and / or documentation of a national ID number, a government-issued identification card with a picture, or a passport.

5.3 SANCTIONS SCREENING

All Supplier personnel must be screened, against the United States Department of the Treasury’s Office of Foreign Assets Control (“OFAC”), Specially Designated Nationals and Blocked Persons (“SDN”) list and the list of regions and jurisdictions subject to sanctions imposed by the United States (“U.S. Sanctions”). OFAC lists are publicly available at this website: https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx.

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.

5.4 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.

*Applicable to suppliers whose personnel has access to Citi systems/networks AND/OR unescorted access to Citi premises (Such personnel would be required to have a GEID, and be registered in Citi’s Non-Employee Management System)
*Also applicable for Suppliers that access/process/store/manage Citi Confidential or Higher Information
5.5 **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.

5.6 **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.

5.7 **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.

5.8 **Drug Screening**
Where legally permissible, Suppliers must ensure that its personnel complete a drug screening test prior to commencing the assignment with Citi. At a minimum, the drug screen must be a "5-panel" test, which tests for the presence of amphetamines, cannabinoids (THC), cocaine, opiates and phencyclidine (PCP). Positive results are to be adjudicated and are sufficient to deny assignment, whether results are received prior to or after the commencement of work, except for where not allowable by local law.
Certain Supplier personnel may be asked to complete a drug screening test during their assignment because of the requirements of the position (e.g., drivers, pilots) or for other reasons in accordance with local laws and regulations.

5.9 **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 [here](#).

5.10 **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.
6 EXPENSES

6.1 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.

6.2 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;
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. Non-compliant requests will not be reimbursed.
7 INFORMATION SECURITY (IS)

*Applicable to Suppliers that access/process/store/manage 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

7.1 Overview

This Section provides minimum requirements for Citi’s Suppliers, who store, process, manage or access Citi Information and/or host Citi applications, regarding the information protection controls that are expected by Citi to ensure that information is protected in accordance with applicable legal and regulatory requirements and the highest industry standards (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 terms and conditions of a Contract.

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

7.2 Information Security Policy & Governance

Suppliers must have documented information security policies and standards. The policy governance must include clearly defined roles and responsibilities, annual review and update of policies and standards, to be consistent with the state of technology, industry standards, legal and regulatory requirements.

7.3 Organization of Information Security

7.3.1 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.

Currently, the following are the only recognized 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 Restricted 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.
7.4 Management commitment to information security / assessments

*Applicable to Suppliers who store, process, manage, or access Citi information classified as Confidential or higher and/or host a Citi-branded Internet-facing application

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

2. Supplier must regularly perform assessments of its business operations and related controls against its information security standards, policies and procedures. The periodic assessments must include, at a minimum:
   a. Assessment of the processes that the Supplier uses to ensure compliance with 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.

3. Issues that have been identified as a result of any Information Security risk assessment must be documented and tracked to closure.

4. If Supplier’s Information Security management function is relocated across country borders, the Supplier must obtain Citi’s documented approval prior to such relocation.

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

6. 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.

7. If Supplier hosts a software or website that contains Citi Information or is Citi branded, periodic vulnerability assessments must be performed in accordance with the Citi’s System Security Testing (SST) Standard and any material issues identified during the assessment must be remediated within the timeframes specified by the Citi SST Standard.

8. If connectivity to servers and / or Information Systems on the Citi internal network is required, then Supplier is required to notify their primary Citi business contact so that the current connectivity process can be followed.
9. The Supplier must promptly notify the appropriate Citi contact of any unauthorized access or acquisition or loss or corruption or deletion of Citi Information or any other compromise to Information Systems used to store, process and / or transmit Citi Information.

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

11. The Supplier must ensure that all sensitive data is masked on screen and on paper (including e.g., monitoring, exception and regulatory and other reports).

12. The Supplier must restrict printing, recording or copying of sensitive data, including by '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.

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

14. 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.

15. The Supplier has a process in place to retrieve all assets when an employee or non-employee is terminated or resigns.

### 7.5 External Parties – Sub-Contractor Information Security Risk

1. 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:
   a. A management approved subcontractor information security assessment process is in place and it covers all steps from assessment initiation through issue management.
   b. 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.
   c. 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.

### 7.6 Asset Management

#### 7.6.1 Responsibility for Assets

1. **Inventory of assets**
   a. 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.
   b. 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.

2. **Protection of assets**
   a. Supplier must be responsible for protecting all Citi Information under its control.

3. **Access and Acceptable Use of Assets**
a. Supplier must ensure accountability of its Users’ activity in a manner consistent with industry practices.
b. User access to personal external Internet e-mail accounts must be restricted from the Supplier’s global network where Citi Information resides.

7.6.2. Information Classification & Handling

1. Information Classification

   a. Citi classifies information per the following Information Classification:

<table>
<thead>
<tr>
<th>Information Classification</th>
<th>PII Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>RESTRICTED</td>
<td>Blank or Yes</td>
</tr>
<tr>
<td>CONFIDENTIAL</td>
<td>Blank or Yes</td>
</tr>
<tr>
<td>INTERNAL</td>
<td>Blank or Yes</td>
</tr>
<tr>
<td>PUBLIC</td>
<td>Blank or Yes</td>
</tr>
</tbody>
</table>

   b. PII Attribute: Personally identifiable Information (PII) can be categorized in any data classification. Appropriate controls must be applied commensurate to the risk level of PII within those classifications.

   c. Authentication is a separate classification with its own requirements and is completely independent of other Information Classifications.

2. Information labelling and storage

   a. 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.

   b. 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.

   c. 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 should 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.

   d. 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 e-mail applications).

3. Information handling procedures

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

   b. 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.

7.6.3. Media Handling

1. Management of removable media

   a. 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.

b. 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.

c. 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.

d. Removable media must be inventoried.

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

2. Disposal of Media

a. 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.

b. 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:

   i. For media that stored information classified as Confidential or higher the tool must complete three passes of the media.

   ii. Degauss the media.

   iii. Destroy the media physically to make it unreadable (i.e. shredding, crushing the drives)

c. 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.

d. 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.

7.7 Cryptographic Controls

7.7.1 Encryption Requirements

Third Party Encryption Requirements for Citi information classified as Confidential or higher:

1. Data transmitted between Citi and the Citi third party must be encrypted end-to-end using as Secure-FTP or other approved Citi tools/standards. To support external file exchanges the approved network security protocols are Transport Layer Security (TLS) and SSH-2 (Secure Shell v2).

2. TLS features authentication, key management and encryption. TLS 1.2 is Citi standard and connections between CDNs and client browsers are supported by TSL 1.2 or TLS 1.3

3. SSH-2 features authentication & key management and it must be used to support external file exchanges

4. Additional Third Party Encryption Requirements for Citi information classified as Confidential PII or higher:
   a) Data persistently stored in the Citi third party environment must be fully encrypted using industry acceptable tools and key strength. To this end, the approved Symmetric encryption algorithm is AES (Advanced Encryption
Standard) with a minimum key size of 128 or 256 bits. It is to be used with NIST approved mode of operation only. AES must be used for data processed and/or stored inside or outside Citi premises. ECB and CBC mode is prohibited for external connections.

b) In the same context, the approved encryption protocols are ECDSA (Elliptical Curve Digital Signature Algorithm) and ECDH (Elliptic Curve Diffie Hellman).

c) For both ECDSA and ECDH the minimum key size is 384 bits which must be used for data processed and/or stored outside Citi premises

d) POLY and SHA-256 are acceptable/approved standards for all hash-function applications. It includes:
   i. In all cases the number of iterations should be set as high as can be tolerated for the environment while maintaining acceptable performance
   ii. SHA-2 family (SHA-224, SHA-256, SHA-384, SHA512, SHA-512/224 and SHA512/256)
   iii. SHA-3 family (SHA3-224, SHA3-256, SHA3-384, and SHA3-512) See FIPS 202
   iv. POLY-1305 See RFC8439

e) For password validation and storage, the approved key derivation functions are PBKDF2 (Password Based Key Derivation Function 2), Bcrypt and Scrypt.

f) PBKDF2 is recommended and must use a minimum iteration count of 10000 with at least 16 byte salt

g) For Bcrypt and Scrypt the minimum number of rounds/cost factor is 10

h) In all cases the number of iterations should be set as high as can be tolerated for the environment while maintaining acceptable performance.

For Citi third parties approved by the Citi BAO to use subcontractors, the above transmission and persistent storage requirements also apply to the subcontractor.

In addition to the above encryption requirements, additional criteria is defined for the following environments:

1. **External Individual Email**: Encryption requirement for individual emails containing Citi Information with a Citi Information Classification of Confidential (non-PII) between Citi and Supplier, where the Supplier is not permitted to use Citi-approved end-to-end encryption software or tools per regulation and/or Supplier policy, may be fully met through transport encryption (e.g., gateway-to-gateway encryption via Transport Layer Security (TLS)).

   a. The approved secure E-mail protocols are IBE (Identify-Based Encryption), MTLS (Mutual TLS) and DKIM (Domain Keys Identified Mail)

   IBE features encrypted email and must be used within Citigroup customer facing solutions and secure e-mail and eDelivery systems only

   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

   DKIM features authentication and key management and is for use with vendors, partners and clients
b. For exchanging authentication and authorization information, the approved security protocol is SAML v2.0. All new implementations of SAML must be at revision 2.0

2. **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.

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

### 7.7.2 Key Management

1. Industry standard cryptographic algorithms and minimum key lengths must be implemented for encryption.

2. Certificates and keys must be changed periodically and have a stated expiration period that does not exceed the guidelines below, as per the Citi Key Management Standard:

<table>
<thead>
<tr>
<th>Type of Key</th>
<th>Maximum Usage Timeframe</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private Signature Key</td>
<td>3 years</td>
</tr>
<tr>
<td>Public Signature Key</td>
<td>Several years (depends on key size)</td>
</tr>
<tr>
<td>Symmetric Authentication Key</td>
<td>2 Years</td>
</tr>
<tr>
<td>Private Authentication Key</td>
<td>2 Years</td>
</tr>
<tr>
<td>Public Authentication Key</td>
<td>2 Years</td>
</tr>
<tr>
<td>Symmetric Data Encryption Keys</td>
<td>2 Years</td>
</tr>
<tr>
<td>Symmetric Key Wrapping Key</td>
<td>2 Years</td>
</tr>
<tr>
<td>Symmetric and asymmetric Random Number Generator (RNG) Keys</td>
<td>Upon reseeding</td>
</tr>
<tr>
<td>Symmetric Master Key</td>
<td>1 year</td>
</tr>
<tr>
<td>Private Key Transport Key</td>
<td>2 Years</td>
</tr>
<tr>
<td>Public Key Transport Key</td>
<td>2 Years</td>
</tr>
<tr>
<td>Symmetric Key Agreement Key</td>
<td>2 Years</td>
</tr>
<tr>
<td>Private Static Key Agreement Key</td>
<td>2 Years</td>
</tr>
<tr>
<td>Public Static Key Agreement Key</td>
<td>2 Years</td>
</tr>
<tr>
<td>Private Ephemeral Key Agreement Key</td>
<td>One key-agreement transaction</td>
</tr>
<tr>
<td>Public Ephemeral Key Agreement Key</td>
<td>One key-agreement transaction</td>
</tr>
<tr>
<td>Symmetric Authorization Key</td>
<td>2 Years</td>
</tr>
<tr>
<td>Private Authorization Key</td>
<td>2 Years</td>
</tr>
<tr>
<td>Public Authorization Key</td>
<td>2 Years</td>
</tr>
</tbody>
</table>

a. Change of key does not need to match the key expiration stated.

b. Keys must be refreshed or rotated prior to expiration to accommodate periods of change, scheduling conflicts and system freezes.

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

4. Suppliers utilizing any form of cryptographic mechanism must use industry standard key management tools and techniques.
7.8 Access Control

7.8.1 Access Control Policy
In order to protect all Controlled Information Systems used to store, access, manage, process, or transmit Citi confidential or higher Information from unauthorized access, the supplier must manage the provisioning of logical access to all systems and applications; controls should 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 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.

7.8.2 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.

7.8.3 User Identification and Authentication

1. All Supplier controlled Information Systems must authenticate the identity of users or systems accessing these platforms prior to initiating a session or transaction where Citi Information may be accessed.
2. All users must be:
   a. Uniquely identified or mapped to the technology platform by a User ID.
   b. Authenticated to the technology platform using a method of authentication - supplier should contact its primary business contact for current approved methods.
   c. All use of shared authentication infrastructure (e.g., Single Sign-on, Reduced Sign-on and other shared authentication services) must be in accordance with the authentication requirements; Supplier should contact its primary business contact for current approved methods.
3. User authentication for external connections:
   a. Remote access to Information Systems used to store, process, manage, and / or transmit Citi Information must be protected from unauthorized use.
   b. If Supplier permits individuals to access its network remotely, 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, Citrix, etc.).

7.8.4 Management of Privileged Access Rights
1. The supplier must maintain an inventory of all privileged and administrative accounts.
2. The direct login to a privileged Functional ID must be granted through a temporary privileged access process.
3. Persistent privileged access may be granted to a user on a Controlled Information System used to store, process, manage, and/or transmit Citi Information only when all of the following conditions are met:
   a. The justification for persistent access is documented as part of the approval.
b. The user’s manager and the information owner / delegate of the Controlled Information System approve the access.

4. Temporary privileged access to Controlled Information Systems must follow a documented password / account release process that:
   a. Requires the requester to be on a pre-approved authorized users list or have an approval at the time of use.
   b. Requires documented justification in a change/problem ticket before access is granted.
   c. Includes an independent review of the activity performed with the access.
   d. Includes a process to revoke / remove the access after a pre-defined period of no more than 24 hours.
   e. 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

5. When logged in with a privileged ID, administrators are prohibited from accessing e-mail, web browsing or performing any function except for that which privileged use was approved.

7.8.5 Review of User Access Rights
1. Supplier must implement a documented process to review, verify and delete unnecessary user entitlements to Controlled Information Systems used to store, process, 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. The entitlements for all privileged non-fixed Functional IDs on Production / CoB Information Systems must be reviewed annually by the ID owner / delegate.
5. The authorized user list for privileged Functional IDs on Production/CoB Information Systems must be reviewed on a quarterly basis by the ID owner(s)/delegate(s).
6. Following a function change by an employee, the supplier has 21 days to perform an access and entitlement review and remove access to Citi data if no longer required for their new function.

7.8.6 User Responsibilities – Password Use
1. User static passwords must never be shared or written down.

7.8.7 System and Application Access Control
1. Secure Log-on Procedures
   a. Login IDs associated with a static password must be locked out after a maximum of six (6) consecutive failed login attempts.
   b. 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.

2. Password Management System
   a. User static passwords must never be displayed on the screen in clear text.
   b. Interactive Privileged Functional ID passwords must not be hardcoded in clear text.
c. Passwords must contain a minimum of eight (8) characters, which must contain both letters and numbers, and be case sensitive.

d. 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).

e. All static passwords must be changed every 90 calendar days at a minimum. Note also:
   i. All authentication systems must enforce a login inactivity/non-use control that should not exceed 100 days if technically feasible. Disabled logins may be re-enabled by the user or another authorized function.
   ii. The authentication Process must ensure that the same password is not used within at least the last six (6) changes.

3. **Use of System Utilities**

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

4. **Session Time-Out**

   a. Re-authentication or login must occur for all Users of a Controlled Information System used to store, process and / or transmit Citi Information.

   b. 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.

5. **Input Data Validation**

   a. Suppliers must have controls in place to protect against online security threats (i.e., cross-site scripting, SQL injection, etc.)

   b. Input validation must be implemented for all Internet and intranet applications.

7.8.8 **Termination of User Access**

1. Upon termination or resignation, user access or entitlements that could allow access to Citi confidential or higher data (user login to Desktop/Active Directory, Single Sign-on (SSO), email, One Time Password (OTP) tokens and remote access) must be removed by the end of the next business day.

2. If an employee has access to Citi owned and administered systems, Citi is notified immediately upon function change or termination of that employee.

7.8.9 **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. All Supplier-managed laptops and all desktop machines used to store, process and / or transmit Citi Information, using remote access where there is local storage / processing of information with a Citi Information classification of confidential or higher, must be encrypted using an encryption tool that meets industry standards

2. Remote connections must only be established through approved remote access solutions that employ multi-factor authentication.

3. 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.

4. 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.
5. 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 should be in place:
   a. Citi Data is prevented from being downloaded to the personal device outside of a company-managed solution.

Remote access solutions such as Terminal Services, VMware Horizon and Citrix must be configured to disable clipboard sharing and Drive Mapping over Blast, PCoIP, RDP and ICA protocols.

7.9 Physical and Environmental Security

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

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

7.9.3 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.

7.10 Operational Security

7.10.1 Operational Procedures and Responsibilities
1. Supplier must have a documented Secure System Development Life Cycle (S-SDLC) in place, in adherence to Citi’s minimum standards, if the Supplier provides software development services to Citi.
2. Supplier must have a documented Change Management process.
3. Supplier must have a documented Capacity Management process that meets relevant industry standards.
4. Where applicable, Supplier must ensure that the Development, Test and Production environments are all physically and/or logically separated from one another.

7.10.2 Protection from Malware
1. 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 etc.) and must implement preventive, detective and recovery controls to protect against such threats.
Supplier must:
a. 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.
b. Have security settings in place to prevent end users from disabling the anti-virus/anti-malware and scheduled scans.
c. Have centrally managed, automated procedures for configuring and updating anti-virus and anti-malware software
d. Processes are implemented for identifying and addressing non-compliant computers where the anti-virus signatures or scan engines are outdated.

2. **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 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:

a. 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. Signed Mobile Code with expired certificates must be removed from production.

7.10.3 **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:
   a. Updates to financial transactions
   b. Updates to Confidential PII data
   c. Updates to Restricted data
   d. Updates to Authentication data
5. Session artifacts (IP address at minimum or other pertinent information), such as unique device ID must be captured, when technically feasible, and logged for Citi facing applications (websites and mobile applications) to support fraud investigations. These artifacts must be captured for Citi transactions and for Citi account opening activity. Information must be captured so the session artifact can be linked to the transaction or account opening.
6. Significant 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.)

7.10.4 Protection of Log Information
1. Supplier must ensure that access controls are present to preserve the integrity of audit trails:
   a. During initiation and shutdown
   b. In storage and during transmission
2. To prevent unauthorized modifications to the audit logs, supplier must ensure that logs cannot be overwritten or modified by the system users whose activity they track.
3. Supplier must define maintain and comply with retention period for log data that complies with the Citi Records Management Policy and all applicable legal and regulatory requirements,
4. The clocks of all relevant information-processing systems within an organization or security domain must be synchronized with an accurate time source.

7.10.5 Monitoring System Use
1. The following events must be captured, logged and reviewed directly or through an automated review process:
   a. All system alarms associated with a firewall or IDS / IPS generated security event
   b. Significant ISA events as noted in Section Audit Logging with the exception of:
      i. Removal of entitlements from user, role or profile.
      ii. Where Information Security Administration activity is executed by an automated workflow / fulfillment system that has end-to-end integrity controls.
   c. All updates to critical resources as identified in the secure standard build.
   d. All interactive activity performed by privileged functional IDs or temporary ID

7.10.6 Log Correlation and Review
1. When a logged event triggers an alert, the event is reviewed, follow up actions and investigation are pursued--if 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 adjusts the configuration of their SIEM or log analytic tool to improve the identification of actionable events.

7.10.7 Secure Configuration
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.
1. Supplier must incorporate information security procedures in its processes and procedures for the selection, development and implementation of applications, products and services.
2. Supplier must have a secure build procedure for all systems where Citi information is stored, processed and/or transmitted.
3. Supplier must maintain a secure image or template for all systems.
4. All default user accounts and passwords are removed and/or changed from vendor-supported systems, network devices, and applications.
5. New system deployments or systems that have been compromised are configured using an approved image or template.
6. Any change to be made to a secure configuration is approved by management via a change management process.
7. When changes occur to the secure configuration, there is a notification process that includes follow up and corrections.
8. The secure build procedure must include tools to support automated configuration checks of the security/standard build settings at the time of production deployment

7.10.8 Control of Operational software
1. Supplier must ensure that:
   a. 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.
   b. A documented process is implemented that specifies the time periods within which all approved security patches and configurations are applied.
2. Regardless of any separate maintenance agreement between Supplier and Citi, Supplier must ensure that software developed for Citi and governed under a license agreement:
   a. Does not require use of versions of non-supported software with known vulnerabilities.
   b. Is updated and patched as required in a timely manner.
3. Open source application software used to process Citi information should be acquired from established suppliers and should be supported.

7.10.9 Vulnerability and Threat Management
The supplier must implement a Vulnerability Management process that includes:
1. Discovery and management of vulnerabilities in all assets that can be used to process, store, access or transmit Citi confidential or higher data.
2. The requirement for at least monthly scans using a tool that discovers instances of the occurrence of currently known vulnerabilities.
3. Ranking of vulnerabilities with remediation timelines based on the severity.
4. The requirement for testing vulnerability fixes prior to full production deployment.
5. An emergency process for remediating critical vulnerabilities.
6. If the supplier host Citi confidential or higher data on Internet-based applications and infrastructure, there should be an annual Vulnerability Assessment "Pen Test" completed by the supplier or an external party that specializes in these type of assessments.
7. 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.
7.11 Communications Security

7.11.1 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. This includes information in transit across the network.
2. Information with a Citi Information Classification of Confidential or higher must not be persistently stored on a system in an Internet-facing Demilitarized Zone (DMZ).
3. With regard to networks used to access, store, manage, process and/or transmit Citi Information, Supplier must ensure that:
   a. Only Wireless Local Area Networks (WLANs) or other wireless device solutions that include reasonable controls to prohibit unauthorized access (PEAP-TLS, EAP-TTLS, etc.) may be connected to networks that contain Citi Information.
   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.
   d. All Citi branded Internet applications and services hosted at Supplier sites must have Citi-approved anti-DDoS (Distributed Denial of Service) services or comparable controls validated by Citi.
   e. 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)

7.11.2 Segregation in Networks
1. 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).
2. During an emergency event, Supplier must be able to filter access between portions of the network to reduce the impact from network Security Events (e.g., port filtering during a virus outbreak).
3. Remote Access and Host Security must implement group-based access controls (e.g., staff, sub-contractors) to limit access to network resources in the Supplier network. At the host level, access control may be done at the group or individual level.

7.11.3 Equipment identification in Networks
1. Technology platforms must identify and authenticate peer technology platforms commensurate with the IS Risk Levels of the interaction and other mitigating controls.
2. 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.
3. 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.

7.11.4 Web Browsing
The 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.

For employees who have access to Citi confidential or higher data:
1. All URL requests must be logged.
2. 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.
3. Access to sites that can expose the environment to malware or attack should be blocked.
4. Attempts to access sites that are deemed non-business related must be blocked.
5. 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.
6. 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.

7.11.5 E-mail
The supplier has 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.

7.11.6 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 7.7 (Policy on the use of cryptographic controls).

7.12 Information Systems Acquisition, Development and Maintenance

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

7.12.2 Online transactions
   1. Where applicable, Supplier must have Information Systems that use dynamic passwords or digital certificates to validate the credentials.
   2. All Certificates’ lifetimes must be replaced at least once every two (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;
         In all these cases, Supplier should contact its primary business contact for the current requirements.
7.12.3 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 an “Availability” of High, logs captured according to Section 10.7q (Audit logging) must be reviewed by the Supplier on a sampled basis. The reviews may be based on an appropriate risk-based sampling methodology.

4. The review must validate changes that are part of the temporary privileged access were made as intended.

7.12.4 Information Leakage

1. Supplier must have documented Secure Coding Standard in place that prevents information leakage, including:
   a. Detailed system information (e.g., server type and technology).
   b. Stack traces and exception errors that reveal directory tree structure and the underlying database type.

7.12.5 Protection of test data

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

7.12.6 System acceptance

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

7.13 Information Security Incident Management

7.13.1 Reporting Information Security Events

1. Supplier should report any Security Incident that compromises or endangers the confidentiality, integrity, or availability of Citi data, or data for which Citi has a custodial obligation, or the information systems housing said data; regardless of how, who (Citi personnel or a Citi vendor or partner), or where (on or off Citi property) the incident occurred. Examples of Information Security Incidents (SIRTs) include:
   a. Misusing of Citi information, in any media or format
   b. Unauthorized access (physical or electronic) to Citi Information
   c. Communication of sensitive Citi Information to unauthorized individuals
   d. Unauthorized modification of data
   e. Sharing Passwords
   f. Computer intrusion (e.g., malware attacks, attacks on Citi’s Internet sites)
   g. Distributed Denial of service (DDoS) attacks
   h. Data destruction
   i. Loss of Citi data in any medium

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

7.13.2 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.

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

7.14 Data Leakage Prevention (DLP) Requirements

1. The 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 the Web.
   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.

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.

7.15 Information Security Training and Awareness Requirements

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.
1. The supplier must have a well-documented Information security training and awareness program in place.
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. The 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.
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>Look up and secure Citi Information after normal work hours and anytime Supplier is away from designated workspace.</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 “Lock Computer”. If a Supplier is using a laptop to view Citi Information, Supplier must ensure that such laptop is secured via cable or security locks to the base unit during work hours and locked securely away after normal work hours.</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>

*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*