

Truist Third Party Information Security Specifications V5.1

	Specification Description	NIST Reference
Subcontractors and Supply Chain	The supplier must provide written notification (notation within a SOW or similar contractual documentation) prior to permitting a subcontractor to process, transmit, store or access Truist confidential information.	N/A
	Supplier must maintain an effective vendor management program to provide oversight on sub-contractors engaged to provide services to Truist.	N/A
	In cases where a primary Supplier sub-contracts services to other parties, the 4 th parties must be subject to the same security requirements agreed upon with the primary Supplier.	N/A
	Direct access and connection from a subcontractor into Truist environment is not allowed unless explicitly approved and agreed by Truist in a formal agreement i.e. SOW or similar contractual documentation.	N/A
Incident Response	Upon discovery of a security incident, at its own cost, Supplier must: - Promptly notify Truist within the allotted timeframe per contract terms. - Use containment measures to mitigate any future potential harm to Truist or Supplier's ability to provide services to Truist. - Begin a thorough investigation of the security incident, including any root cause(s) analysis. - Promptly remediate the security.	PR.IP-9
		DE.AE-2
		DE.AE-3
		DE.AE-4
		DE.AE-5
		DE.DP-4
		RS.AN-2
		RS.AN-4
		RS.MI-1
		RS.MI-2
		RS.RP-1
		RS.CO-2
		RS.IM-2
	Supplier must regularly communicate the progress of its incident investigation to Truist and promptly cooperate to provide Truist with any reasonably requested information in a timely manner.	RS.CO-2
		RS.CO-3

		RS.CO-4
		RS.CO-5

	Supplier systems that access, process, or store or allow the access, processing, or storage of Truist confidential information must be managed using the principle of least privilege. - Access Roles must: - Be approved by Access Role reviewer prior to being created. - Follow a standardized naming convention and descriptions. - Reflect the current access Entitlement levels.	PR.AC-1
		PR.AC-4
		PR.PT-3
		PR.IP-1

- Maintain the principle of Least Privileged Access and prevent toxic access combinations upon creation.
- Be reviewed at least annually to ensure principle of Least Privileged Access and Separation of Duties.

All SaaS applications must be federated (SAML or LDAP) to Truist's Enterprise IDP (currently, Azure Active Directory). This will enable the SaaS application to meet Truist password standards.

Public information, such as Truist email address, User Principal Name or Federation ID must be used as part of the identity assertions.

Password requirements are a full set of the requirements set by the most updated version of National Institute of Standards and Technology (NIST) SP 800-63B-3 and SP 800-63-3, or alternatively, the following set of requirements:

- Multi-Factor Authentication (MFA) is required when a User attempts to perform any of the following activities:
 - Privileged access to an application.
 - Access to privileged account credentials.
 - Access to the Truist network from outside the Truist network. (e.g., VPN access, VDI access)
 - User access should be based on data classification.
- All business privileged accounts require MFA. (Knowledge Based Questions are NOT accepted as valid MFA.)
- Supplier passwords should adhere to the following requirements:
 - Software Tokens issued by Supplier must:
 - Not be installed on Supplier-owned or managed laptops and workstations.
 - Software tokens must be unique to a single User identifier.
 - Passwords should support ASCII characters (including spaces), must have a minimum age of one day, and not allow for dictionary words.
 - ***Eight (8) characters minimum*** (no maximum limit).
 - Complexity Rules: At least 3 out of 4 of the following: 1 upper case, 1 lower case, 1 special character, 1 number.
 - Suppliers must implement common password blocking capabilities.
 - Passwords and credentials must be hashed or encrypted at rest, and in-transit.
 - Passwords and User IDs must be communicated separately to the user.

○ Initial and temporary passwords and PINs must be unique when constructed. ○ User passwords must have a minimum age of one (1) day. • User accounts must be locked after ten (10) consecutive unsuccessful login attempts. • Auto unlock after thirty (30) minutes. • Password reuse must be prohibited for at least 10 passwords. • Supplier privileged user passwords must be at least twelve (12) characters long, must be complex and the complexity must contain at least three (3) of the four (4) different attributes from the following list: ○ Upper case letters, Lower case letters, Numbers, Special characters. • Supplier passwords used in accessing the Truist network environment are considered privileged accounts. • Password complexity and rotation rules must be followed. • Human interactive authentication must be automatically locked after a maximum of 15 minutes of inactivity. • Human interactive authentication must be re-authenticated at least every 12 hours to ensure privileges have not changed.	
Supplier group or shared accounts/passwords are prohibited and must be managed in an approved password vaulting.	PR.AC-6
• Password owners must: ○ Not share or reveal passwords. ○ Not embed or hard code passwords within the source code of an application, on the command line, or within a configuration file. ○ Disable default passwords to applications and systems.	PR.AC-7
Supplier must not use default passwords.	PR.AC-7
Two-factor authentication must be used for all Supplier user accounts with privileged or elevated rights to systems that host, process or could reasonably access Truist confidential information.	PR.AC-6
	PR.AC-7
Two-factor or Multi-Factor Authentication (MFA) must be used for Supplier personnel remote access to Supplier systems and networks that host or process Truist confidential information.	PR.AC-6
	PR.AC-7
Supplier must perform user access reviews at least twice annually:	PR.AC-1
• Access Roles must: ○ Be approved by Access Role reviewer prior to being created.	PR.AC-6
	PR.AC-7

	○ Follow a standardized naming convention and descriptions. ○ Reflect the current access Entitlement levels. ○ Maintain the principle of Least Privileged Access and prevent toxic access combinations upon certain. ○ Be reviewed at least annually to ensure principle of Least Privilege and Separation of Duties.	PR.PT-1
	• Application and system owners must ensure Entitlements are created with Least Privileged Access based on roles and responsibilities.	
	Supplier must perform privileged user access reviews at least quarterly:	PR.AC-1
	• Access Roles must: ○ Be approved by Access Role reviewer prior to being created. ○ Follow a standardized naming convention and descriptions. ○ Reflect the current access Entitlement levels. ○ Maintain the principle of Least Privileged Access and prevent toxic access combinations upon certain. ○ Be reviewed at least annually to ensure principle of Least Privilege and Separation of Duties. • Application and system owners must ensure Entitlements are created with Least Privileged Access based on roles and responsibilities.	PR.AC-6
		PR.AC-7
		PR.PT-1
	Supplier must have effective procedures in place for provisioning and deprovisioning Supplier user access. Privileged accounts must be deprovisioned after no more than 24 hours.	PR.AC-1
		PR.AC-4
		PR.AC-6
		PR.AC-7
		PR.IP-11
	For all systems under Supplier control (including systems hosted for Truist as part of the provision of Services), Supplier is responsible for logging and monitoring access-related activity:	PR.AC-3
	• If Supplier personnel will access Truist networks or Truist hosted systems, end user access logs must be retained for a minimum of 12 months. • Otherwise, end user access logs must be retained for a minimum of 90 days. • Privileged user access logs must be retained for a minimum of 12 months.	PR.AC-6, PR.PT-1

	Supplier must apply Data Loss Prevention (DLP) specifications to monitor and block unauthorized egress of sensitive data across known egress channels.	N/A
	Supplier must centrally log, maintain, and review Data Loss Prevention (DLP) generated events in a central repository to identify instances of potential or confirmed sensitive data exfiltration.	N/A
	Supplier must test the efficacy of DLP policies before deploying into the production environment.	N/A
	Supplier must maintain an activity baseline to help detect and block anomalous data exfiltration events.	N/A

Encryption and Data Loss Prevention

Supplier must provide alerting mechanisms to notify key stakeholders, including incident responders, and Truist within 24 hours [timeline is subject to change, but aligns with other requirements in the addendum] of a reasonably suspected or actual compromise of sensitive Truist information.	N/A
Supplier must document cryptographic processes and controls to include: a) key issuance b) key maintenance c) key transfers d) key revocation/destruction	N/A
Supplier portable media and devices that contain Truist confidential information must be encrypted, using Advanced Encryption Standard (AES) 256-bit encryption or NIST approved encryption algorithm; all key lengths must utilize 256-bit key length or greater.	PR.DS-1
	PR.DS-2
	PR.DS-3
	PR.PT-2
Supplier must encrypt Truist confidential information in Supplier's control, at rest and in transit, using Advanced Encryption Standard (AES) 256-bit encryption or NIST approved encryption algorithm; all key lengths must utilize 256-bit key length or greater.	PR.DS-1
	PR.DS-2
	PR.PT-4
Supplier must have effective encryption key management procedures that must at a minimum include: • Limited access to the key vault. • All access to the key vault must be logged and maintained for a minimum of 12 months. • Keys must be distributed only to known and authorized parties and to the fewest number of parties possible. • All encryption keys must have an expiration date and must be rotated prior to the expiration date. • Keys generation materials must be destroyed and rendered unrecoverable immediately upon key creation. • Activities including key generation, distribution, access, storage, and rotations must be logged.	PR.DS-2
Supplier must notify Truist of any reasonably suspected or actual compromise of any encryption key used to protect Truist confidential information.	N/A
In cases where Truist confidential information is in a multi-tenant environment, encryption keys unique to Truist must be used, unless specifically authorized by Truist in either the contract or SOW.	PR.DS-1
	PR.PT-4

Supplier must inventory all certificates, including certificate owners and fingerprints. Additionally, the Supplier must ensure that all PKI keys are issued by an Enterprise Certificate Authority, or a publicly trusted Certificate Authority.	N/A
PKI Key Pairs must be securely generated, updated, and maintained.	N/A

	Certificate-based authentication must check for the following: • Signature by a trusted Certificate Authority (CA). • Expiration date of the certificate. • Distinguish name (DN) in the subject. • Authorization to gain access to the Application and/or resource. • Revocation status of the certificate.	N/A
	Supplier must establish a mutually accepted "chain of custody" process using dual control for transferring ownership of an encryption key between individuals, servers, or organizations. This process should ensure that documentation supporting the ownership transfer is also appropriately transferred.	N/A
	Keys must only be issued to authorized custodians, and the supplier must ensure that users implementing cryptographic capabilities are informed and trained according to their roles and responsibilities.	N/A
	Supplier must use a cryptographic key of 4096 bits or longer for digital code signing services.	N/A
	Encryption keys must be rotated every 24 months or less.	N/A
	Suppliers must agree to permit Truist to perform a non-intrusive (without logon or active Truist control of Supplier Systems) annual audit of Supplier's adherence to this Information Security Exhibit and the Security Standards.	ID.BE-1
		ID.SC-4
	In addition to any due diligence questionnaire-based assessments Truist may send during the year or queries based on potential security issues, the Supplier must cooperate with security assessments by answering questions and by providing access to: • Relevant policies, procedures, and documentation. • Knowledgeable personnel. • Covered supplier systems. • Other information relevant to assessing the security of Supplier's environment. • Where possible, those same elements for any subcontractor; and any additional information at the reasonable request of Truist.	PR.IP-8
		RS.CO-2
	To the extent Supplier utilizes a site-to-site connection to Truist's network or provides services that use Internet-facing sites and/or applications, Truist may request Supplier to provide an executive summary of any third	ID.BE-1
		ID.RA-3

Security Assessment	party vulnerability scan reports related to such site(s) and/or application(s) as part of the security assessment. Should Supplier not have such a report, Supplier must agree, at its exclusive cost, to engage a mutually agreed-to third party to perform vulnerability testing on covered Supplier systems at Supplier's sole expense.	ID.RA-6
		ID.SC-4
		DE.AE-3
		DE.AE-4

	For environments where Truist is not Supplier's exclusive tenant, supplier will take all reasonable steps to provide all necessary permissions and access rights to supplier Systems and Supplier facilities used in the performance of services, to perform a nonintrusive assessment (without logon or active Truist control of supplier systems - "show not share") without the need to disclose information or provide access to particular systems (or environments within the system) that would violate Supplier's confidentiality obligations to co-tenants.	N/A
	Suppliers must agree that Truist (or at its election, an agent or an independent third party agreed to by the parties) may conduct additional security assessment(s) during the same year if any of the following conditions are met: • An audit identified a material audit finding. • Truist identifies or reasonably suspects a violation of the Exhibit or a Security Incident. • Material changes such as new or substantial modification to services supplied by Supplier resulting in identified increased risk. In addition to any related due diligence assessments, and upon Truist's request relating to risks, threats and events sourcing from Supplier's external-facing assets or any threat intelligence feeds;; Truist will engage	DE.AE-2
		ID.BE-2
		ID.SC-2
		ID.SC-3
		ID.SC-4
		DE.AE-3
		DE.AE-4
		DE.AE-5
		RS.AN-1

	Supplier to provide actionable information of regarding the identified risks, threats, or events (brought to the Supplier's attention) to understand and request applicable remediation steps taken regarding the identified critical risk to Supplier's supply chain security to prevent potential impact to the Supplier's network, services provided to Truist, and to Truist Confidential Information.	RS.AN-2
		ID.BE-1
	Truist will notify Supplier in the event that a security assessment reveals a material risk related to the services or software provided. Supplier must promptly remediate any assessment findings within five (5) days after notice or develop a mutually agreeable plan designed to promptly remediate any assessment findings. In the event that Supplier disagrees with such finding Supplier must work in good faith to negotiate a mutually satisfactory mitigation strategy.	PR.IP-12
		ID.BE-1
		ID.BE-2
		ID.RA-6
		ID.SC-3
		DE.AE-3
		RS.IM-2
	Truist must retain security assessment rights throughout the term of the agreement and for as long as Supplier retains any Truist confidential information or connection to Truist's network.	ID.SC-4
	Supplier must acknowledge that the requirements of the relevant section are separate and distinct from any assessment or questionnaire resulting from Supplier's participation in consortium led assessments (e.g. KYP3) other questionnaire-based assessments or other due diligence effort from Truist.	N/A

Continuous Monitoring	Truist reserves the right to engage our higher risk suppliers to investigate status of their external security hygiene through use open-source intelligence tools or curated threat hunting and leverage any related security alerts to engage supplier for any remedial efforts needed.	N/A
	Truist or Truist client's sensitive information is prohibited from being ingested into a third-party vendor's open-source Gen AI tool.	N/A

	Supplier must restrict access to Truist Confidential Information and Supplier Systems hosting Truist Confidential Information or providing service to Truist, to a need basis using the principle of least privilege. Unless otherwise specifically approved in a SOW, supplier must maintain the operating environment supporting the Truist Service(s) (including any Truist Confidential Information) in a segregated state from supplier internal environments and those environments used by/for supplier's other clients such that only authorized supplier personnel or subcontractors providing services to Truist may gain access. • Access Roles must: ○ Be approved by Access Role reviewer prior to being created. ○ Follow a standardized naming convention and descriptions. ○ Reflect the current access Entitlement levels. ○ Maintain the principle of Least Privileged Access and prevent toxic access combinations upon creation. ○ Be reviewed at least annually to ensure principle of Least Privileged Access and Separation of Duties.	PR.AC-3
	All remote access to Truist's Network or Truist's hosted systems by Supplier personnel is subject to written approval from Truist prior to accessing Truist Systems and Truist Confidential Information. Such approval must be in the form of a duly executed SOW or from a Truist Senior Vice President (or the current equivalent title) or above at the time of remote access invocation. In the event of a pandemic or other such disaster recovery event, Supplier, upon request from Truist, must provide a remote access personnel status report to Truist for all supplier personnel connecting to Truist systems.	PR.AC-3
	Supplier must use two-factor authentication for (i) all accounts with privileged or elevated access rights to systems or applications hosting or processing Truist confidential information, and (ii) any remote access by supplier to systems or Truist confidential information.	PR.AC-7

Access Controls and Multi-Factor Authentication (MFA)	Supplier must perform adequate logging and monitoring of access related activities; Access to these logs should be reviewed in a timely manner and logs must be restricted to only those personnel that have a need to know.	PR.PT-1
	Supplier must collect and evaluate security events using appropriate tools including an effective Security Information and Event Management system (SIEM).	DE.AE-2
		DE.AE-3
	Supplier Personnel are required to use a Truist or Supplier-controlled device when accessing Truist Systems and Truist Confidential Information.	PR.AC-2
	Supplier-controlled devices must be continuously monitored when accessing Truist Systems and Truist Confidential Information.	PR.AC-4
		PR.AC-7
	No Truist data may be copied to or stored in a Supplier device unless previously agreed to in a SOW or similar binding agreement.	N/A

	Supplier devices must be hardened in accordance with the Level 1 Center for Internet Security Benchmark profile or equivalent security standard and applied via group policy objects.	N/A
	Supplier devices must have a mandatory login, screen inactivity/locking timeout (fifteen (15) minutes).	N/A
	Supplier Virtual Private Network ("VPN") must be configured to be "always on." If not technically feasible, each hardened device must have On and Off Net Proxy with a reasonable level of controls (i.e. content filtering, DLP, etc.).	PR.PT-4

	VPN software must be installed utilizing NIST approved cryptographic schemes and algorithms with at least 2048-bit and/or 256-bit encryption as applicable.	PR.PT-4
	When connecting to the Truist network, supplier personnel must be limited through network capabilities (e.g., firewall, routing, etc.) to connect only to the designated Truist environment. Split tunneling is prohibited.	PR.PT-3
	Supplier devices must have supplier-managed, commercial grade data loss prevention control software designed and must be configured to prevent and detect data leaks of Truist confidential information on in-scope systems and networks.	PR.DS-5

	Any removable media (CD/DVD drive, USB port(s), etc.) must be adequately configured to prevent any storage device from connecting. In cases where a business requirement is determined that requires such connection of removable media, the Supplier must ensure the following: • An effective policy that covers such deviations is in place: a) Deviations must be time limited. b) Deviations must be reviewed at least annually. • Deviations are documented and approved by the CISO or equivalent senior leader within Supplier's organization. • All controls protecting the connections from ingress/egress of data or malware are in place and effective.	PR.PT-2
	Supplier personnel remote access must be restricted to the United States, or to such other country locations identified and agreed to by Truist in the SOW or Master Service Agreement and must be documented in the inherent risk assessment.	ID.RA-4
		ID.RA-5
Viruses and Malware	Supplier must have anti-virus/malware protection enabled on all servers and workstations that access, process, or store Truist proprietary or Truist Confidential information.	PR.DS-8
	Supplier anti-virus/malware tools must be centrally managed and updated at least daily.	PR.DS-8

	Supplier anti-virus/malware tools must periodically perform endpoint scans and promptly remediate any findings.	ID.RA-3, ID.RA-1
		DE.CM-8
		PR.DS-8
		DE.CM-4
	Supplier work product that is intended to be installed on Truist systems must not contain mechanisms that will harm Truist systems, cause Truist systems to become inaccessible to Truist, or permit any Supplier to access Truist proprietary or Truist Confidential information or systems.	DE.CM-5
	Supplier must ensure that its Vulnerability Patch processes and procedures are designed and implemented to industry-best practices or as specified in InfoSec Addendum.	N/A
Network Security	Supplier networks must be managed, monitored, and controlled to protect Truist Confidential Information. Supplier shall implement multilayered network security infrastructure that provides continuous monitoring, restricts unauthorized network traffic, and detects and limits the impact of attacks, including: (i) firewalls or other filtering devices, and (ii) intrusion detection systems (“IDS”) and/or intrusion prevention systems (“IPS”) configured and maintained to ensure optimal protection, log suspicious, or unauthorized network traffic patterns, and to alert Supplier Personnel of actual or suspected compromises. Network traffic shall be appropriately segregated with routing and access controls separating traffic on internal networks from public or other untrusted networks. High-risk administrative ports (i.e., Telnet) and ports on externally facing systems that are not required for business functions should not be accessible from the Internet. Information systems, network devices, and applications shall be configured and deployed using a secure baseline (hardened), maintained to address known vulnerabilities, and with extraneous ports/services disabled. Supplier must restrict the connection times of idle/inactive sessions on information systems, applications, and network devices, and terminate inactive sessions. Supplier shall perform regular vulnerability assessments and scans of multilayer network security infrastructure to identify potential vulnerabilities and weaknesses. Identified vulnerabilities must be remediated within defined service level agreement (SLA) timelines aligned with Truist standard.	PR.PT-4
		DE.CM-1
		PR.AC-5
		PR.DS-2, ID.RA1, PR.IP-3
		PR.IP-12

If the Supplier has a connection to a Truist network (intermittent or static) where the Supplier's equipment is used to enable the connectivity, then the supplier must twice annually or upon request from Truist, attest that the connectivity equipment is updated and patched according to their own internal process and procedures and ensuring all applicable critical security patches are applied promptly.	DE.CM-8
Out-of-Band Communications ("OOB"). If the Supplier requires out-of-band communications to manage their equipment and/or software, they must ensure one or more of the following: • Dial-back: when management access is required, the user dials the number associated with the device. The device answers, hangs up, and then calls a pre-configured number. • Caller-ID: will only accept calls from specific, pre-defined di numbers. • Secure Modem: requires a specific, pre-configured modem at each end of the connection. • Touch Tone password device: an inline device that requires a distinct password to be entered using touch-tone numbers. • Access Management for OOB: all access transactions, whether successful or not, should be logged to a separate logging facility. Any unsuccessful access should cause an immediate alert to be generated and forwarded to a real-time (or as close to real-time as practical) monitoring system. This system can range from a console display at a 24x7 staffed operations center to email or pager notification. Assessment logs should be reviewed on a regular basis.	PR.PT-4
	DE.CM-1
	PR.AC-5
	PR.DS-2
Supplier must have an effective asset inventory that identifies all organizational informational and technology assets. Supplier must additionally assign owners to assets and track lifecycle details of the assets. Supplier must define asset classification and integrate asset inventory with vulnerability management process to track all assets and can be assessed for vulnerabilities throughout their lifecycle.	PR.AC-1
	PM-5, ID.AM-2, ID.AM-5

	The supplier must twice annually or upon request from Truist, provide details of the make and model of VPN client/router/server and ensure that EOL and EOS hardware is not leveraged for initiating connections to Truist environment. Or attestation that device is not EOL or EOS and properly patched.	N/A

	Supplier must use industry standard tuned and configured Web Application Firewall (“WAF”) or similar technology that is designed to protect known injection attacks, broken authentication, sensitive data exposure, XML external entities (“XXE”), broken access control, security misconfigurations, cross site scripting (“XSS”), and insecure deserialization, or other technologies that provide similar web application security at runtime.	ID.RA-1
		ID.RA-3
		PR.DS-5
		DE.CM-6
	Prior to implementation of WAF the host must be scanned and remediated using accepted industry standard tools for security vulnerabilities (e.g. Open Web Application Security Project and Open Web Application Security Project Top 10). Post implementation of WAF, the host shall be scanned at defined frequency or whenever there are major changes. Scan results must be shared with Truist at defined interval or when requested. Additionally, the WAF must be peer-reviewed to ensure correct configuration.	N/A
	Supplier's WAFs must be included in the vulnerability scanning (i.e. WAS scans) and vulnerabilities must be promptly remediated. Scanning must be at a frequency that is appropriate for the relevant application, technology, and data risk.	ID.RA-1
		ID.RA-3
		ID.RA-5
		PR.DS-5
		DE.CM-6
		DE.CM-8

Web - Enabled Applications

Externally facing websites maintained by a supplier on behalf of Truist must be configured with the following account and password controls and must meet the full set of requirements set forth in the most updated version of National Institute of Standards and Technology (NIST) SP 800-63B-3 and SP 800-63-3, or alternatively, the following minimum set of requirements:

- Password complexity must be implemented for all accounts.
- Complexity must include at least three of the four different attributes from the following list:
 - a) 1 upper case, 1 lower case, 1 special character, and 1 number
- Periodic forced password changes no more than every ninety (90) calendar days.
- Account lockout after no more than ten (10) failed attempts in thirty minutes.
- Prohibit group or shared accounts / passwords.
- Prohibit use of default passwords.
- Password history of at least 10 remembered: NIST Standard 800-44V2 states that the organization password policy would be appropriate for this control.
- Minimum password age of one day.
- Periodically check passwords against known password dictionaries.
- Passwords should support all ASCII characters (spaces included).
- Passwords must not be shortened during processing.

PR.AC-1

	Externally facing websites must additionally implement and maintain accepted industry standard account and password management controls, including: • First-time and One-time password login expiration after no more than 24 hours. • Prohibiting user IDs, passwords and personal data from being displayed in a URL. • Storing user passwords and reset/forgotten security questions in an encrypted manner. • Re-authentication is required after no more than 15 minutes of inactivity. • Prohibiting the storage of passwords or personal data in persistent local storage (caches, etc.) or in any cookies, JavaScript, or other web tracking technology.	
	Applications hosted by a Supplier for Truist teammate logon must be restricted to Truist owned networks unless otherwise specified in the terms of the contract. Where technically applicable, applications hosted by a Supplier for Truist teammate logon must support single sign-on (SSO).	N/A
Software Coding and Application Development Security	Supplier must implement appropriate technical and organization measures to ensure the delivery of secure code (e.g., the OWASP Application Security Verification Standard), including strong configuration management, application security testing, runtime exploit prevention and ensuring no vulnerable open-source code.	PR.DS-7
		PR.IP-2
		PR.IP-3
	Supplier's development will not be complete until the security of the code and application has been demonstrated via a security report. Must comply to Truist standard. Such security report must be provided by Supplier and reviewed and accepted by Truist.	PR.DS-7
		PR.IP-2
	Supplier must not store, transmit, access, or display any production data within non-production systems designated as development, quality assurance, or test.	PR.DS-1
		PR.DS-2
		PR.DS-5

		PR.DS-7
--	--	---------

	Supplier must have a secure software development policy that applies to all development practices.	N/A
	Truist must reserve the right to test (including, - Dynamic Application Security Testing- DAST-, Static Application Security Testing- SAST- & Penetration Testing- PEN-) all supplier software used in connection with the Services. When not feasible, supplier must, at its own expense, provide to Truist an independent verification of test execution, results and remediation plans where applicable.	N/A
	Prior to delivery, Supplier software must not have an open CVE with a CVSS of 8.0 or higher in score, based on the then-current CVSS version.	N/A
	Supplier must notify Truist within 24 hours when Supplier becomes aware of any zero-day vulnerabilities in software they provide.	N/A
	For any Supplier providing software that meets the definition of Critical Software, Supplier will provide these additional security specifications: Upon request, Supplier must provide a Software Bill of Materials (SBOM) that will describe at a minimum: - List of all Open Source and Supplier Components (In SPDX or Cyclone DX format). - License for Open Source and Supplier Components. - Versions and Patch Status for Open Source and Supplier Components. - Support and User/Development community supporting the software.	N/A
	Supplier must provide a method to authenticate their software that is immutable, such as code signing.	N/A
	Application Security Third Party Security Requirements: SAST/SCA - All applications with source code must be scanned. - Applications must remediate all critical and high vulnerabilities prior to production.	N/A

Vulnerability Management	Application Security Third Party Security Requirements: DAST • All web applications must be scanned. • Applications must remediate all critical and high vulnerabilities prior to production release.	N/A
	Application Security Third Party Security Requirements: APIs • All critical APIs must be scanned: ◦ Prior to deployment to production ◦ At least annually • In scope APIs must remediate all critical and high vulnerabilities prior to production release.	N/A
	Vulnerability (Infrastructure) Management Third Party Security Requirements: • Infrastructure discovery scans must be done monthly and reconciled with an asset inventory. • Infrastructure vulnerability and Configuration scans must be conducted on a weekly basis against the full Organizational network. • Mainframe Vulnerability scans must be conducted on a Quarterly basis. • Threat and vulnerability intelligence sources must be used for identification of known vulnerabilities. • The Organization must calculate and assign severity scores or ratings for all findings, vulnerabilities, configuration compliance gaps. • Vulnerability risk scores must be used to prioritize remediation of identified findings, vulnerabilities, and configuration compliance gaps. • All discovered vulnerabilities must be stored in a system of record for review for a minimum of 3 years. • The Organization must disposition and remediate all vulnerabilities and configuration gaps based on the organizations risk appetite.	N/A
	Penetration Testing Requirements: • Third Party must perform Penetration Testing on all applications in support of or provided to Truist. ◦ Third Party must engage an independent party to conduct Penetration Testing. • Penetration Testing must occur on an annual basis.	N/A

Security Awareness and Training	Supplier must provide information security awareness training at least annually to all its personnel with access to Truist confidential information or Truist systems that are materially covered in the security requirements of this baseline and must at a minimum include: • Phishing training. • A method to test assimilation of topics covered. • Require remedial and/or disciplinary actions for failed simulated tests.	PR.IP-11
---------------------------------	--	----------

PCI/Payment Card Data	As applicable, Supplier must comply with PCI Security Standards (i.e. PCI PTS, PCI PA-DSS, PCI DSS, PCI P2PE), as well as obtain and maintain applicable third party PCI Security Standards certification. Supplier is responsible for the security of Truist cardholder data that supplier possesses or otherwise stores, processes, or transmits on behalf of Supplier and will furnish evidence of current PCI Security Standards certification for the relevant services. Supplier will conduct PCI Security Standards required quarterly network scans on the in-scope environment via an Approved Scanning Supplier (as defined by PCI Security Standards), whose use is hereby consented to by Truist. To the extent that Supplier is performing Services that are “in scope” of Payment Card Industry standards (PCI Service Provider or Merchants) acting on behalf of Truist must have their PCI scope assessed by a Qualified Security Assessor (“QSA”) with an annual Report of Compliance (“ROC”). Supplier shall provide upon request and on a defined rolling basis, evidence of compliance (i.e. an Attestation of Compliance, Certification of Compliance, etc.).	N/A
-----------------------	---	-----

	If applicable, physical security requirements, controls, and measures must be in place for Truist assets at Supplier facilities, in compliance with Truist Corporate Security requirements. Any exceptions or changes must be communicated and approved by Corporate Security.	PR.AC-2
		PR.DS-3
		DE.CM-2
	Supplier must implement and maintain administrative, physical, and technical safeguards designed to protect Truist confidential information and covered Supplier systems from unauthorized access, acquisition, disclosure, destruction, alteration, unavailability, misuse, or damage which must meet or exceed relevant and currently accepted industry standards, including but not limited to the NIST Cybersecurity Framework, the International Organization for Standardization (ISO) 27001/2 Series of Standards, and the Control Objectives for Information and related Technology (COBIT) Standards.	PR.AC-2
		PR.DS-8
		PR.IP-7
		DE.AE-1
		DE.CM-1
		DE.CM-2
		DE.CM-3

Physical Security Requirements	Any Supplier personnel who access any Truist System or any facility of Truist or one of its affiliates during or in connection with performance of services must comply with Truist's information security and physical security policies and procedures, as presented to personnel at time of access.	PR.IP-5
		PR.IP-11
		DE.CM -3

Data Return or Destruction	Third Parties must agree to return or securely dispose of Truist Information Assets upon termination of the third-party relationship. Supplier must provide evidence (e.g. certificate of destruction) of data destruction in line with termination of vendor relationship with Truist and/or in line with retention policies as previously agreed upon.	PR.DS-3
		PR.IP-6

	Supplier must automatically and on a regular basis, perform complete, comprehensive, and resilient backups of (i) Truist Confidential Information in Supplier's custody or control and (ii) systems and information necessary to the performance and availability of the Services (such as system data needed to operate Supplier's Systems).	ID.SC-5
		PR.DS-4
		PR.IP-4
		PR.PT-5
		ID.BE-4
	Truist restricted information as well as systems and information necessary to the performance and availability of the services must be backed up at least daily.	PR.DS-4
		PR.IP-4
		PR.PT-5
	Supplier must segregate backups from production environments and maintain them in a manner that is resilient to physical disaster and malicious attack (e.g., ransomware), including using encryption and	ID.BE-4
		ID.BE-5
		PR.IP-4

Business Continuity	ensuring that backups have at least one offline backup destination (i.e., not accessible via a network connection).	PR.PT-5
	Supplier must conduct regular testing of backup restoration and must have and test an effective plan to ensure rapid and successful recovery of data and services in the event of a disruption to the performance or availability of the Services resulting from a system outage or security incident.	ID.SC-5
		PR.IP-4
		PR.IP-9
		PR.IP-10
		PR.PT-5
		RS.MI-1
		RS.MI-2
		RC.RP-1

	When applicable, Supplier must deploy user entity behavior analysis (UEBA) tools to detect, identify, and track anomalies on Supplier's systems, equipment, and end user work behaviors.	IR-4 Incident Handling; IR4(13). Behavior Analysis, - Analyze anomalous or suspected adversarial behavior in or related to [Assignment: organization defined environments or resources].
--	--	--

Offshore Security

Supplier must require and maintain stricter language in their acceptable use policy and non-disclosure agreements (NDA) executed for remote workers and provide these details upon request for offshore employees working on related Truist projects.	CA-3 Information Exchange; CA-3(a), PL-4 Rules of Behavior, PS-4 Personnel Termination, PS-6 Access Agreements
When applicable, Supplier must deploy on Supplier's systems and equipment, geolocation related tracking capabilities, which log and monitor traffic patterns and Supplier must regularly review logged information to validate approved remote work location status.	SR-4 Provenance; SR-4(1) Identity; (2) Track & Trace; (3) Validate as Genuine and Not Altered, CM-8 System Component Inventory; CM-8(8) Automated Location Tracking
Supplier must provide personnel with privacy screens and require its use when working in a hybrid mode (i.e. away from Supplier designated buildings.	MP-1 Policy & Procedures, MP-2 Media Access, MP5 Media Transport, MP-6 Media Sanitization, PE4 Access Controls for Transmission, PE-5 Access Control for Output Devices

Supplier must deactivate off network browsing for hybrid workers. (i.e. workers not specifically performing functions within an ODC).	System and Comm Protection, SC-1 Policy & Procedure; SC-2 Separation of System and User Functionality, SC2(1) Interfaces for Non-Privileged Users
Supplier must establish policies and procedures that dictate work from home privilege approval processes, tailored to data classification levels and service criticality, and maintain a current and historical list of approved hybrid workers. Upon request, Supplier must provide Truist with an up-to date copy of such rosters.	System and Communication Protection: SC-1 Policy and Procedures; SC-2 Separation of System and User Functionality, SC2(1) Interfaces for Non-Privileged Users; SC-3 Security Function Isolation, SC-3(5) Layered Structures

When applicable, Supplier personnel, using Supplier devices and equipment, must first connect to Supplier's internal network, via an established Virtual Private Network (VPN), and, where applicable, prior to connecting to any Truist Citrix (Virtual Desktop Infrastructure (VDI)) gateway or environment.	System and Information Integrity: SI-1 Policy & Procedures; SI-4 System Monitoring, SI4(4) Inbound and Outbound Communications Traffic; SI-4(5) System-Generated Alerts, SI-4(6) Restrict Nonprivileged Users, SI-4(7) Automated Response to Suspicious Events, SI-4(13) Analyze Traffic and Event Patterns
Disable USB ports in devices including connectivity for charging.	N/A
Minimum security standards for home routers.	N/A
Access management groups for offshore or hybrid resources.	N/A

Cloud Security	Upon request from Truist Supplier must agree to provide independent verification (e.g. Federal Risk and Authorization Management Level Medium, CSA Certification for cloud deployments, HiTrust, SOC 2 Type II, etc.) in addition to other or at Truist's discretion, in place of, full security assessments.	N/A
	The Supplier must provide a list of Cloud hosted applications or services that are used in support of the service(s) offering to Truist.	N/A
API Security	Must have API Specifications that contain well-defined schemas and security definitions for each API.	
	Ensure API validates inputs against the API schema. Validation includes rejecting: malformed parameters, unexpected parameters, and artificially large payloads.	
	APIs must sanitize output.	
	Legacy or deprecated APIs must be removed within 90 days of deprecation notice.	
	APIs must implement strong authentication mechanisms. (i.e., OAuth / mTLS)	
	An API Gateway is used for integrations outside of the boundaries of an application for APIs that are developed specifically for Truist by a third party.	

	API Gateway must be configured to validate authentication and authorization.	
	A WAF must be deployed in front of the API Gateway to provide an additional layer of security for all external facing APIs.	
	API must not contain sensitive fields in the URL and must not write sensitive data in the logs.	

For questions or to report a concern, please contact Truist Cyber Incident Management via either of the following:

Email: CyberIncidentManagement@Truist.com

Telephone: 833-920-1772