



○ ○ ○ ○



Third-Party Cybersecurity Requirements Guideline

○ ○ ○ ○

June-2026



Third-Party Cybersecurity Standard (TPCS)

General Requirements - Control Guidelines

Controls 1 to 33

Scope	This document covers only the General Requirements controls 1 to 33 from the Third-Party Cybersecurity Standard.
Purpose	For each control, the Control Guidelines provide the evidence package expected to demonstrate compliance.
How to use	Collect and submit the listed evidence for each applicable control in the self-assessment report template. Mark a control non-applicable only with documented justification and approved compensating controls, where applicable.
Note	The guidance is written generically for a third-party environment. Adjust evidence names, tools, owners, and procedures to match the actual operating model and contractual requirements.

Control Guidelines Table

Control #	Control Statement	Control Guidelines
TPC1.1	Third party must ensure legislative and regulatory compliance, which should include, as a minimum, continuous compliance with all laws, regulations, instructions, decisions, regulatory frameworks and controls, and mandates regarding cybersecurity and data privacy in KSA and/or other applicable national regulations.	• Provide an approved legal/regulatory compliance policy or procedure covering cybersecurity and data privacy obligations in KSA and any other applicable jurisdictions. • Provide compliance obligations register or regulatory matrix listing applicable laws, regulations, instructions, regulatory frameworks, controls, and mandates. • Provide the latest compliance review, self-assessment, or audit report showing compliance status, identified gaps, remediation actions, owners, and due dates. • Provide evidence of monitoring and updating applicable regulatory requirements, such as a regulatory update tracker, legal review record, or compliance review minutes.
TPC1.2	Third Party must develop, approve and communicate an Acceptable Use Policy (AUP).	• Provide a copy of the approved Acceptable Use Policy (AUP). • Provide evidence that the AUP is approved by authorized management and version-controlled. • Provide evidence that the AUP was communicated to employees, contractors, and relevant users, such as email communication, intranet publication, training records, or acknowledgement records.
TPC1.3	Third party must establish, maintain, and communicate Cybersecurity Policies and Standards that include, at minimum, the following: a) asset management;	• Provide approved cybersecurity policies and standards covering, at minimum, asset management, access management, physical security, secure media disposal/data sanitization, classification and handling of assets/data, incident management, vulnerability and patch management, and business continuity/disaster recovery. • Provide evidence that the cybersecurity policies and standards are maintained, version-controlled, and approved by authorized management.

	b) access management; c) physical security; d) secure disposal of media/sanitization of data; e) classification and handling of assets and data; f) incident management; g) vulnerability and patch management; h) business continuity and disaster recovery.	• Provide evidence that the cybersecurity policies and standards were communicated to employees and relevant third parties, such as publication records, emails, training records, or acknowledgements.
TPC1.4	Third Party must have formal documented process for on-boarding employees (i.e. conducting background checks) and off-boarding employees (i.e. return of assets and removal of access rights).	• Provide the formal documented employee onboarding procedure covering background checks or screening before access is granted. • Provide the formal documented employee offboarding procedure covering return of assets and removal of access rights. • Provide sample completed onboarding records, such as background check/screening evidence and approved access provisioning records. • Provide sample completed offboarding records, such as asset return forms, account disablement evidence, access removal confirmation, or leaver tickets.
TPC1.5	Third Party must obtain a Cybersecurity Compliance Certificate (CCC), or approved certificate, from authorized audit firms in accordance with the requirements set forth in this Standard. Third Parties must submit the CCC to proponent through the established process.	• Provide a valid Cybersecurity Compliance Certificate (CCC), or approved certificate, issued by an authorized audit firm. • Provide evidence that the certificate scope covers the applicable third-party classification, entity, services, and contract scope. • Provide evidence that the certificate was submitted to the proponent through the established process, such as portal submission, email confirmation, or acknowledgement.
TPC1.6	Third Party must renew the CCC (or approved	• Provide the current CCC, or approved certificate, showing issue date, expiry date, and validity period.

	certificate) before it expires.	• Provide evidence that the CCC renewal was completed before expiry or that renewal activities were initiated before expiry. • Provide evidence of submission of the renewed CCC, or approved certificate, to the proponent through the established process.
TPC1.7	Proponent data must only be shared with individuals who are part of the work specified in the contract.	• Provide the data sharing or data handling policy/procedure stating that proponent data is shared only with individuals assigned to the contracted work. • Provide the approved list of personnel authorized to access or receive proponent data, including role or business justification. • Provide access permissions, distribution list approvals, collaboration workspace permissions, or data sharing records showing proponent data is restricted to authorized individuals.
TPC1.8	Third party must have an effective mechanism to maintain an inventory of all information and technology assets, ensuring visibility and accuracy across all technical assets.	• Provide the asset management policy/procedure defining how information and technology assets are identified, recorded, owned, and updated. • Provide the latest asset inventory or CMDB export covering all in-scope information and technology assets. • Provide evidence that the inventory includes key attributes such as asset ID, asset name/hostname, owner, location, asset type, status, and criticality/classification. • Provide evidence of periodic inventory review, reconciliation, or automated discovery to maintain inventory accuracy.
TPC1.9	User authorizations to information technology systems and applications must be managed via a centralized corporate identity and access management solution. Authorizations must be based on: a) identity; b) access control principal - Need-to-Know and Need-to-Use basis; c) least privilege and Segregations of Duties.	• Provide the access management policy requiring centralized corporate identity and access management for in-scope systems and applications. • Provide configuration screenshots, architecture documentation, or system inventory showing systems and applications managed through the centralized IAM, directory, or identity provider solution. • Provide an authorization model, role matrix, or access control matrix showing access based on identity, need-to-know, need-to-use, least privilege, and segregation of duties.

		• Provide sample access request, approval, modification, and removal records from the centralized IAM/access management process.
TPC1.10	User authentication must be granted based on unique authentication credentials.	• Provide the access management policy requiring unique user authentication credentials. • Provide user account listings or screenshots from sample systems/applications showing individual named accounts are used. • Provide evidence that generic/shared accounts are prohibited or formally approved, restricted, monitored, and reviewed where required.
TPC1.11	The following rules must be used for password and authentication code management (where feasible): using long passwords or passphrases between 8 - 64 characters in length; containing lower case characters a-z; containing upper case characters A-Z; containing digits 0-9; containing special characters (e.g. ! @ # \$ % ^ & *, etc.); using multi-factor authentication (MFA) mechanism; vii. not providing password hints.	• Provide the password and authentication code management policy covering password/passphrase length, complexity, MFA, and prohibition of password hints where feasible. • Provide technical configuration evidence from Active Directory, LDAP, identity provider, local security policy, or application settings showing password length and complexity requirements are enforced where feasible. • Provide evidence that password hints are disabled or not used where feasible. • Provide evidence of MFA enforcement where required by this control and related access controls.
TPC1.12	Multi-factor authentication must be enforced on: remote access (including access from the Internet); access to cloud services; access to company email through web/mobile devices; access to internet facing applications; users with privileged accounts.	• Provide the access management or MFA policy requiring MFA for remote access, cloud services, company email through web/mobile devices, internet-facing applications, and privileged accounts. • Provide MFA configuration screenshots or policy exports showing MFA is enforced for the required access types. • Provide MFA compliance or enrollment reports showing covered users and privileged accounts. • Provide approved exception records and compensating controls for any required MFA coverage gaps, where applicable.
TPC1.13	Single sign-on can be used but must be coupled with MFA upon initial login to a system.	• - If SSO is used, provide the SSO policy or configuration standard requiring MFA upon initial login. • Provide identity provider/SSO configuration screenshots showing MFA is enforced at initial SSO authentication.

		• Provide sample login evidence, authentication logs, or screenshots showing MFA is triggered during initial SSO login.
TPC1.14	Third-Party must review user accounts and access rights at least annually.	• Provide the access management policy requiring user account and access rights reviews at least annually. • Provide the latest completed access review records covering user accounts and access rights for in-scope systems and applications. • Provide evidence of reviewer approval/sign-off and remediation actions for access changes, removals, or exceptions identified during the review.
TPC1.15	All Third-Party Technology Assets must be authenticated using secure authentication mechanisms.	• Provide the authentication or access control policy requiring secure authentication mechanisms for all technology assets. • Provide configuration evidence showing secure authentication mechanisms are enabled on in-scope technology assets such as servers, workstations, network devices, applications, and cloud resources. • Provide sample authentication logs, configuration screenshots, or management console reports demonstrating secure authentication is active on selected technology assets.
TPC1.16	All proponent data must be securely returned to the proponent and then deleted from all technology assets at the end of the Data Life Cycle or designated retention period (including backups).	• Provide the data return and deletion policy/procedure covering proponent data at the end of the data lifecycle or designated retention period, including backups. • Provide evidence that proponent data was securely returned to the proponent, such as transfer records, delivery confirmation, or proponent acknowledgement. • Provide evidence that proponent data was deleted or sanitized from technology assets and backups, such as deletion logs, sanitization records, or backup expiry records. • Provide written confirmation or certification to the proponent that the return and deletion activities were completed.
TPC1.17	Technology Assets must be securely disposed at the end of their lifecycle (e.g.	• Provide the secure disposal policy/procedure for technology assets at end of lifecycle, including loaned, donated, destroyed, transferred, or surplus assets.

	loaned, donated, destroyed, transferred or surplused) in accordance with applicable legislative requirements and industry best practices.	• Provide evidence of approved sanitization or destruction methods used before asset disposal, aligned with applicable legislative requirements and industry best practices. • Provide sample asset disposal records, destruction certificates, sanitization certificates, or chain-of-custody records.
TPC1.18	Third Party must encrypt data at rest and in transit using technical mechanisms and cryptographic primitives for strong encryption, in accordance with the advanced level in the KSA National Cryptographic Standards (NCS-1:2020) and industry-approved encryption algorithms.	• Provide the encryption policy/standard requiring encryption of data at rest and in transit using strong encryption aligned with KSA NCS-1:2020 advanced level and industry-approved algorithms. • Provide technical evidence of data-at-rest encryption, such as disk, database, file, storage, or cloud encryption configuration screenshots/reports. • Provide technical evidence of data-in-transit encryption, such as TLS/HTTPS, VPN, SSH/SFTP, email encryption, or API encryption configuration screenshots/reports. • Provide evidence of cryptographic algorithms and key lengths used for in-scope systems and data flows.
TPC1.19	Third party must restrict and secure the use of external storage media.	• Provide the external/removable storage media policy defining restrictions, approval requirements, and security requirements for external storage media. • Provide technical configuration evidence showing external storage media is restricted or controlled, such as endpoint device control, USB control, DLP, or MDM policy settings. • Provide evidence that approved external storage media is secured where used, such as encryption configuration or approved device inventory. • Provide monitoring logs, exception approvals, or violation reports for external storage media usage, where applicable.
TPC1.20	Third Party must implement Sender Policy Framework (SPF), Domain Message Authentication Reporting (DMARC) and DomainKeys Identified Mail (DKIM) technology on the mail server.	• Provide DNS records and mail server/security gateway configuration showing SPF is implemented. • Provide DNS records and mail server/security gateway configuration showing DKIM is implemented. • Provide DNS records and mail server/security gateway configuration showing DMARC is implemented.

		Provide validation test results, screenshots, or reports confirming SPF, DKIM, and DMARC are active for the third-party private email domain.
TPC1.21	Third Party must inspect all incoming emails originating from the Internet using anti-spam protection.	- Provide email security gateway, mail server, or cloud email protection configuration showing anti-spam inspection is enabled for incoming Internet emails. - Provide anti-spam policy/rule configuration showing actions such as block, reject, quarantine, or mark as spam. - Provide sample reports or logs showing incoming Internet emails are inspected by anti-spam protection.
TPC1.22	Third Party must inspect all email attachments with signature analysis before allowing the attachments.	- Provide email security gateway, mail server, or cloud email protection configuration showing all email attachments are inspected before being allowed. - Provide evidence that attachment inspection uses up-to-date signature analysis, such as anti-malware engine/signature update status. - Provide sample attachment scanning logs, blocked/quarantined attachment reports, or alerts.
TPC1.23	Third Party must use a private email domain. Generic Public domains, such as Gmail and Hotmail, must not be used.	- Provide the AUP or email usage policy requiring use of the third-party private/corporate email domain and prohibiting generic public domains such as Gmail and Hotmail for business/proponent communications. - Provide evidence of the approved private/corporate email domain, such as domain ownership, DNS MX records, or email service configuration. - Provide evidence that personnel were informed of the private email domain requirement, such as communication, training, or acknowledgement records.
TPC1.24	Third Party must ensure that Microsoft Office Macros in any files originating from external sources (such as internet downloads and email attachments) are automatically blocked.	- Provide the endpoint or Microsoft Office security policy requiring macros from external sources to be automatically blocked. - Provide GPO, Intune, Microsoft 365 Apps, Office Trust Center, or equivalent configuration evidence showing macros from Internet downloads and email attachments are blocked. - Provide test evidence, screenshot, or alert showing an externally sourced macro file was blocked.

TPC1.25	Third Party must synchronize all technology assets with an authorized time source e.g., NTP server.	• Provide the time synchronization/NTP policy or standard identifying authorized time source(s). • Provide configuration evidence showing in-scope technology assets synchronize with an authorized time source. • Provide sample screenshots, command output, or management console reports showing NTP/time synchronization status for selected assets.
TPC1.26	Event logs must be protected from alteration, disclosure, destruction, and unauthorized access and unauthorized release.	• Provide the log management policy/standard requiring event logs to be protected from alteration, disclosure, destruction, unauthorized access, and unauthorized release. • Provide access control/RBAC configuration showing log access is restricted to authorized personnel. • Provide technical evidence of log protection, such as centralized log forwarding, retention controls, backups, immutable/WORM storage, or integrity protection. • Provide sample evidence that log access, changes, deletion, or release is controlled and recorded.
TPC1.27	Firewalls must be configured and enabled on all endpoint devices.	• Provide the endpoint firewall policy requiring firewalls to be configured and enabled on all endpoint devices. • Provide centralized configuration evidence such as GPO, MDM, EDR, endpoint security, or firewall management settings showing endpoint firewalls are enabled. • Provide endpoint firewall compliance report or sample screenshots showing firewalls are enabled on endpoint devices. • Provide approved firewall exception records and remediation evidence for non-compliant endpoints, where applicable.
TPC1.28	Third Party must inspect all HTTP and HTTPS traffic from Internet facing (External) applications using Web Application Firewall (WAF).	• Provide an application/network architecture diagram or inventory showing all Internet-facing external applications in scope. • Provide WAF configuration screenshots or exports showing HTTP and HTTPS traffic inspection is enabled for Internet-facing applications. • Provide routing, DNS, reverse proxy, or load balancer evidence showing Internet-facing application traffic passes through the WAF.

		• Provide WAF logs, alerts, or reports showing inspected, blocked, or allowed HTTP/HTTPS requests.
TPC1.29	Third Party technology assets must be protected with signature based up-to-date virus and malware protection software.	• Provide the virus/malware protection policy requiring signature-based, up-to-date protection on technology assets. • Provide anti-virus/anti-malware or endpoint protection management console report showing coverage of in-scope technology assets. • Provide sample endpoint/server screenshots showing the protection agent is installed, active, and updated. • Provide signature/version update reports or logs showing malware protection is up to date.
TPC1.30	Before implementation to the production environment, security patches must be tested or have measures implemented to ensure back-out or recovery is possible.	• Provide the patch management policy/procedure requiring security patches to be tested before production deployment or supported by back-out/recovery measures. • Provide sample security patch change records showing pre-production testing, approval, and production deployment details. • Provide evidence of back-out or recovery measures used for production patching, such as rollback plans, backups, snapshots, restore points, or recovery procedures. • Provide post-deployment validation evidence confirming patch implementation or recovery readiness.
TPC1.31	Audit and cybersecurity event logs must be activated on information systems and applications. Logs must capture at minimum the events stated in Appendix C.	• Provide the logging/audit policy or standard requiring audit and cybersecurity event logs to be activated on information systems and applications. • Provide a mapping to Appendix C showing required event types and where each event type is captured. • Provide configuration screenshots or exports showing audit/cybersecurity logging is enabled on in-scope information systems and applications. • Provide sample logs demonstrating capture of required Appendix C event types.
TPC1.32	If Third Party discovers a Cybersecurity Incident, Third Party must (besides its continuous efforts to resolve and mitigate the	• Provide the incident response policy, plan, or procedure requiring continuous mitigation, proponent notification within 24 hours of discovery, and use of the Appendix A incident response process.

	Incident): a) notify proponent within 24 hours of discovering the Incident; b) follow the Cybersecurity Incident Response Process set forth in Appendix A.	• Provide the incident notification workflow, escalation matrix, contact list, or communication procedure showing how the proponent is notified within 24 hours. • Provide the incident reporting template or form used for proponent notification. • Provide sample incident tickets, notification emails, reports, or tabletop exercise records demonstrating the 24-hour notification process.
TPC1.33	Third party must notify proponent when third party employees provided with proponent user credentials no longer requires access. This includes employee being transferred, re-assigned, retired, or no longer associated with the Third Party.	• Provide the policy/procedure requiring notification to the proponent when personnel with proponent credentials no longer require access due to transfer, reassignment, retirement, resignation, termination, or contract end. • Provide the inventory/list of third-party personnel issued proponent credentials, including user ID or access reference, role, manager/owner, and current status. • Provide sample notification emails, tickets, or requests sent to the proponent to revoke or update access. • Provide proponent confirmation, disabled/revoked account evidence, or reconciliation records showing access was removed or updated.