Third Party Cybersecurity Controls Guideline

February/2022

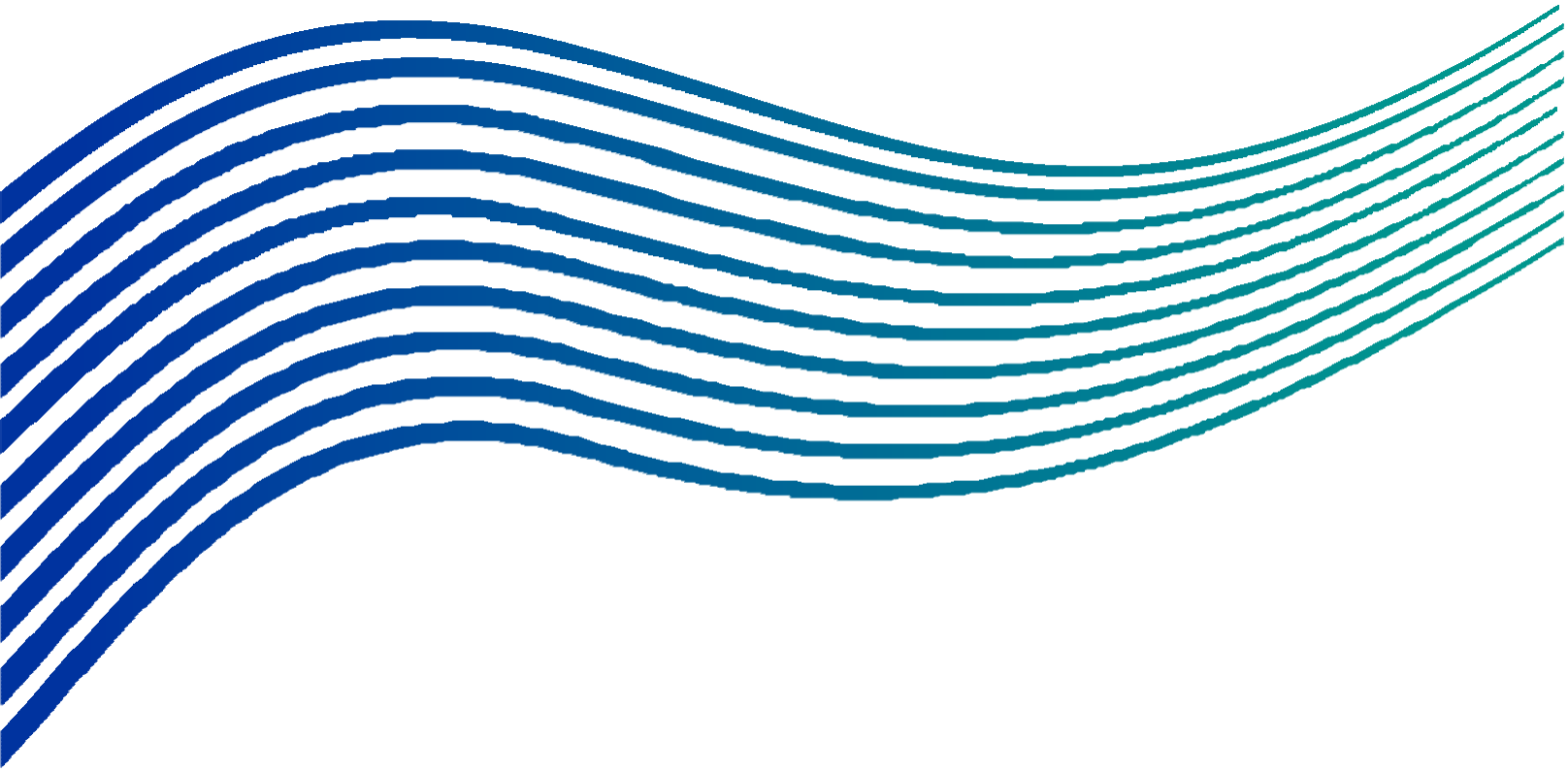

Table of Contents

• Objective

The objective of Third Party Cybersecurity Compliance Certification Program is to ensure all third parties adherence to the cybersecurity requirements in SACS-002 Third Party Cybersecurity Standard by obtaining a Cybersecurity Compliance Certification form an Authorized Audit Firm. This manual will provide the third party with the required guidance to fulfill the cybersecurity controls' requirements for each control. This will ensure that supported, required and comprehensive evidences are provided part of the third party compliance package that will be submitted to authorized audit firm.

• Cybersecurity Controls' Requirement

The cybersecurity controls guidance document must be used as a reference to ensure unified expectations for the evidences to be provided for each cybersecurity control. The guideline must be utilized for remote assessments where third parties must provide a comprehensive assessment package in accordance to all the controls' requirements stated in this document. Moreover, this guideline can be used for on-site assessments where audit firms can verify the evidences against each control's requirements. In case of inapplicability, third party must fill the inapplicability form with required justifications for each inapplicable control.

1. General Requirements

Control #	Control Statement	Controls' Requirements
TPC-1	Third Party must establish, maintain and communicate a Cybersecurity Acceptable Use Policy (AUP) governing the use of Third Party Technology Assets.	- Provide a copy of approved (AUP) - Provide sample of communication regarding sharing (AUP) to employees - Provide different versions of approved and communicated AUP, that shows different releases and updates
TPC-2	Password protection measures must be enforced by the Third Party. The following are recommended measures: - Minimum length: 8 alphanumeric characters and special characters. - History: last 12 passwords - Maximum age: 90 days for login authentication - Account lockout threshold: 10 invalid login attempts. - Screen saver settings: automatically locked within 15 minutes of inactivity.	- Provide technical check evidence to confirm the compliance of the control requirements. - Provide evidence of the password configuration on Active directory to ensure that default settings are not used. If active directory does not exist, provide evidences from the local password policy on sample systems. - Provide a copy of password policy that should comply with the control requirements and technical check findings.
TPC-3	Third party must not write down, electronically store in clear text, or disclose any password or authentication code that is used to access Assets or Critical Facilities. This should be part of Third Party cybersecurity polices.	- Provide a copy of password disclosure policy - Provide a copy of actions taken in case password disclosure happened part of the consequence management

Control #	Control Statement	Controls' Requirements
TPC-4	Multi-factor authentication must be enforced on all remote access, including access from the Internet, to Third Party Company computing resources.	- Provide technical check evidence to confirm that strong authentication is in place on remote users' access (e.g., multifactor) a clear evidence of the Authentication page must be provided. - Provide policies and procedures related to remote users' access policy part of the third party access control policy.
TPC-5	Multi-factor authentication must be enforced on all access to Cloud services utilized by the Third Party, including access to cloud-based email.	- Provide technical check evidence to confirm that strong authentication is in place on cloud access (e.g., multifactor) a clear evidence of the Authentication page must be provided. - Provide policies and procedures related to cloud security policy part of the third party access control policy.
TPC-6	Third Party must inform Saudi Aramco when employees provided with Saudi Aramco user credentials no longer need their access, or are transferred, re-assigned, retired, resigned or no longer associated with the Third Party.	- Provide the third party policy/contract in term of dealing with Saudi Aramco credentials. - Provide a sample of communication (Email) to Saudi Aramco to revoke invalid accounts. - Provide evidence for revoked accounts that are invalid accounts for people who are retired, resigned or no longer associated with the Third Party.
TPC-7	Third Party must require all information systems users to take a yearly mandatory Cybersecurity training that addresses acceptable use and good computing practices. Training must address the following topics: 1. Internet and social media security 2. Cybersecurity Acceptable Use 3. Social Engineering and phishing emails 4. Sharing credentials (i.e. username and password) 5. Data Security	- Provide acceptable use policy and/or training materials to ensure content is adequate. - Provide user training reports and/or documentation to ensure users are trained in accordance with applicable policy, guidance, and/or requirement (e.g., annual cybersecurity training of all employees). - Provide evidences of updating the training materials based on changes in cyber threat environment.
TPC-8	Third Party must inform personnel, in keeping with Third Party Company Policy, that using personal email to share and transmit Saudi Aramco data is strictly prohibited.	- Provide Third Party Company Policy and contract of using personal email. - Provide the Third Party policy / contract ensure third parties are complying with cybersecurity responsibilities defined in contracts and agreements. -Provide related emails communicated to third party's employees to ensure the compliance of this control. - Provide relevant counter measure that third party has taken to comply with the control requirements.

Control #	Control Statement	Controls' Requirements
TPC-9	Third Party must inform personnel, in keeping with Third Party Company Policy, that disclosing Saudi Aramco policies, procedures and standards or any type of data with unauthorized entities or on the Internet is strictly prohibited.	- Provide Third Party policy including contracts and agreements that highlight the prohibited disclosure of Aramco related data. -Provide related emails communicated to third party's employees to ensure the compliance of this control - Provide relevant counter measure that third party has taken in case of disclosing Saudi Aramco Data
TPC-10	All Third Party Technology Assets and Systems must be password protected.	- Provide evidence of related assets management policy that define Technology assets' protection. -Provide evidence of related policy for all third party systems to be password protected.
TPC-11	Third Party Technology Assets and Systems must be regularly updated with operating system (OS), software and applets patches (i.e. Adobe, Flash, Java etc.)	- Provide evidence of patch management policy and procedures - Provide evidence of on sample of workstations to ensure that OS and software are up-to-date - Provide evidence of scheduling and technology used for patch and updates deployment.
TPC-12	Third Party Technology Assets must be protected with anti-virus (AV) software. Updates must be applied daily, and full system scans must be performed every two weeks.	- Provide evidence of the anti-virus installed on endpoint devices - Provide evidence of configuration console of the installed anti-virus software to determine the last updates and full system scan that were performed - Provide evidence of the history of updates
TPC-13	Third party must implement Sender Policy Framework (SPF) technology on the mail server.	- Provide evidence of SPF implementation on the third party mail server.
TPC-14	Third party must enforce Sender Policy Framework (SPF) feature on Saudi Aramco email domains: Aramco.com and Aramco.com.sa.	- Provide evidence of SPF enforcement on Saudi Aramco email domains: Aramco.com and Aramco.com.sa.
TPC-15	Third Party must publish SPF record in DNS server.	- Provide evidence of SPF record on the third party DNS server.
TPC-16	Third Party must inspect all incoming emails originating from the Internet using anti-spam protection.	- Provide evidence of using an anti-spam protection for all incoming emails on the email security appliance.
TPC-17	Third Party must use a private email domain. Generic domains, such as Gmail and Hotmail, must not be used.	- Provide evidence of the third party acceptable use policy (AUP) that highlights the use of the third party private email domain only and prohibit the use of generic domains.

Control #	Control Statement	Controls' Requirements
TPC-18	Third Party must have formal procedures for off-boarding employees. Off-boarding procedures must include the return of assets, and removal of all associated access.	- Provide evidence of the third party termination procedures to determine whether accounts/access are disabled in a timely manner. - Provide samples of the removal of all access to Assets part of the third party Off-boarding procedures.
TPC-19	Assets used to process or store Saudi Aramco data and information must be sanitized by the end of the Data Life Cycle, or by the end of the retention period as stated in the Contract, if defined. This includes all data copies such as backup copies created at any Third Party site(s).Third party shall certify in writing to Saudi Aramco that the data sanitization has been completed.	- Provide evidence of the third party sanitization (data destruction) policies. - Provide evidence of sanitization techniques and procedures are commensurate with the security category or classification of the information or asset and in accordance with organizational standards and policies. - Provide proof (e.g., destruction certificates) that media sanitization is occurring according to policy
TPC-20	Third Party must obtain a Cybersecurity Compliance Certificate (CCC) from Saudi Aramco authorized audit firms in accordance to the third-party classification requirements set forth in this Standard (Section II). Third Parties must submit the CCC to Saudi Aramco through the Saudi Aramco e-Marketplace system.	- Saudi Aramco third parties must obtain a Cybersecurity Compliance Certificate (CCC) from Saudi Aramco authorized audit firms, which provides the adherence to this standard. -In case CCC has been previously obtained, an evidence of certificate submission should be provided.
TPC-21	Third Party must renew the CCC every two (2) years.	- Saudi Aramco third parties must renew the CCC every two (2) years as per the standard requirements. -A copy of latest CCC obtained needs to be provided.
TPC-22	Firewalls must be configured and enabled on endpoint devices.	- Provide evidence of the firewall setting for all third party endpoint devices including related policies for enabling firewalls. - Provide evidence of the firewall being enabled on domain, public and private firewall settings on sample of third party endpoint devices.
TPC-23	If Third Party discovers a Cybersecurity Incident, Third Party must (besides its continuous efforts to resolve and mitigate the Incident): - Notify SAUDI ARAMCO within two (24) hours of discovering the Incident - Follow the Cybersecurity Incident Response Instructions set forth in Appendix A.	- Provide evidence of the third party cybersecurity Incident management policies and procedures that conform with the requirements of this control.

End of General Requirements