





VII. Third Party Cybersecurity Controls

A. General Requirements

Third Parties must comply with all cybersecurity controls specified in this section.

CNTL No.	Control Name
IDENTIFY	
Governance (GV)	
TPC-1	Third Party must establish, maintain and communicate a Cybersecurity Acceptable Use Policy (AUP) governing the use of Third Party Technology Assets.
PROTECT	
Access Control (AC)	
TPC-2	<p>Password protection measures must be enforced by the Third Party. The following are recommended measures:</p> <ul style="list-style-type: none"> - 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.
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 policies.
TPC-4	Multi-factor authentication must be enforced on all remote access, including access from the Internet, to Third Party Company computing resources.
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.
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.
Awareness and Training (AT)	
TPC-7	<p>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:</p> <ol style="list-style-type: none"> 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



CNTL No.	Control Name
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.
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.
Data Security (DS)	
TPC-10	All Third Party Technology Assets and Systems must 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.).
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.
TPC-13	Third party must implement Sender Policy Framework (SPF) technology on the mail server.
TPC-14	Third party must enforce Sender Policy Framework (SPF) feature on Saudi Aramco email domains: Aramco.com and Aramco.com.sa.
TPC-15	Third Party must publish SPF record in DNS server.
TPC-16	Third Party must inspect all incoming emails originating from the Internet using anti-spam protection.
TPC-17	Third Party must use a private email domain. Generic domains, such as Gmail and Hotmail, must not be used.
Information Protection Processes and Procedures (IP)	
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.
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). The sanitization must be conducted in alignment to industry best practices such as NIST 800-88. Third party shall certify in a signed letter to Saudi Aramco that the data sanitization has been successfully completed.
Protective Technology (PT)	
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.
TPC-21	Third Party must renew the CCC every two (2) years.

CNTL No.	Control Name
TPC-22	Firewalls must be configured and enabled on endpoint devices.
RESPOND	
Communications (CO)	
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 twenty-four (24) hours of discovering the Incident - Follow the Cybersecurity Incident Response Instructions set forth in Appendix A.

B. Specific Requirements

Third Parties that may fall under one or multiple class, described in section (II), needs to follow this section specific requirements.



CNTL No.	Control Name	Network Connectivity	Outsourced Infrastructure	Critical Data Processor	Customized Software	Cloud Computing Service
IDENTIFY						
Asset Management (AM)						
TPC-24 	Third Party must have policies and processes to classify information in terms of its value, criticality and confidentiality.	✓	✓	✓	✓	✓
Governance (GV)						
TPC-25	Third Party must establish, maintain and communicate Cybersecurity Policies and Standards.	✓	✓	✓	✓	✓
TPC-26	Third Party must be staffed by employee(s) whose primary responsibility is Cybersecurity. Responsibilities of that personnel must include maintaining the security of information systems and ensuring compliance with existing policies.	✓	✓			
Risk Assessment (RA)						
TPC-27	Third Party must conduct annual external Penetration Testing on its IT infrastructure systems, and internet facing applications.	✓	✓		✓	✓
TPC-28 	Third Party must conduct annual external Penetration Testing on Cloud Computing Service(s) used by Saudi Aramco					✓