



SACS-002


Third Party Cybersecurity Standard

Disclaimer: The contents of this report should be treated by Third Parties as CONFIDENTIAL and is intended solely for the use of the individual or entity to which it is addressed. This report may contain legally privileged information and may not be disclosed or forwarded to anyone else without authorization from Saudi Aramco.

Content

- Definitions and Abbreviations 2
- I. Purpose 5
- II. Scope..... 5
- III. Change Control..... 6
- IV. Conflicts and Deviations..... 6
- V. Revision 6
- VI. Cybersecurity Controls Instructions..... 6
- VII. Third Party Cybersecurity Controls 8
 - A. General Requirements..... 8
 - B. Specific Requirements..... 10
- VIII. Reference 18
- IX. Approval..... 19
- Appendix A - Cybersecurity Incident Response Instructions 20
- Appendix B - Cybersecurity Incident Subsequent Reports and Notifications..... 23
- Appendix C - Auditing Events 26

Definitions and Abbreviations

Term	Definition
Assets	Anything that has value to Saudi Aramco created (intellectual and personal data) or procured data, proposed or executed contracts, agreements, devices, systems, hardware, software, research information, training manuals, operational or support procedures, continuity plans and any facilities that enable the organization to achieve business purposes.
Audit log	A chronological record of system activities. Includes records of system accesses and operations performed in a given period. Examples of auditable events are included in Appendix C.
Compliance Assessment	The practice and activities conducted on processes and systems to evaluate and verify their adherence to the enforced cybersecurity controls in the Standard and the Contract.
Critical Data	Saudi Aramco confidential data that if leaked or lost would result in high risk and adverse impact to Saudi Aramco including but not limited to brand reputational damage, financial loss, operational impact, loss of proprietary information, or loss of competitive advantage.
Content-filtering	The use of a program to screen and exclude users from accessing web pages and services that contain hate-based, pornographic, extremist/militancy, gambling, illegal substances or other objectionable material.
Corporate Network	The Saudi Aramco computing resources and infrastructure, excluding Plant Networks and International Offices Networks.
Critical Facilities	A physical location housing information processing Systems such as data centers, communications closets, or cabling (power, network etc.).
Cybersecurity	The mandatory minimum information security requirements to support the protection of confidentiality, integrity, and availability of Assets.
Cybersecurity Assessment	Cybersecurity Assessment include Risk Assessment, Compliance Assessment, Vulnerability Assessment and forensic analysis. Cybersecurity Assessment is conducted by Saudi Aramco using Saudi Aramco resources to ensure that the Third Party is in compliance with cybersecurity controls in the Standard and the Contract.
 Cybersecurity Incident	Unauthorized access, disclosure, modification or disruption of information, systems and services. Physical incidents include but not limited to: <ul style="list-style-type: none"> • Unauthorized physical access to restricted areas or communication rooms • Theft of Assets
Cybersecurity Policy	The set of laws, rules, directives and practices that governs how an organization protects information systems and information.
Data Life Cycle	The process of managing the flow of data. The cycle includes the management of data from creation and storage to the time when the data becomes obsolete and is deleted.
DMZ	Demilitarized Zone or a perimeter network is an additional layer of security to separate an organization's Local Area Network (LAN) from other untrusted networks such as the Internet and has additional cybersecurity controls to restrict access to other layers in the network.

Term	Definition
Incident Response	A process detailing the steps required to minimize or eradicate Cybersecurity Incident that threatens the confidentiality, integrity or availability of the Third Party's or Saudi Aramco's Assets. A critical component of this process is highlighting the guidelines and procedures for defining the criticality of Cybersecurity Incident, reporting and escalation process, and recovery procedures.
Patch	A piece of software designed to fix operating system or software programming errors and Vulnerabilities.
Penetration Testing	A live test of the effectiveness of security defenses through mimicking the actions of real-life attackers to uncover Vulnerabilities. This includes testing a computer system, network or Web application.
 Public Cloud Computing	A model for enabling on-demand network access to a shared pool of configurable IT capabilities/resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal operation management effort or service provider interaction. It allows users to access technology-based services from the cloud without knowledge of, expertise with, or control over the technology infrastructure that supports them.
Remote Access	Act of utilizing a remote access service, hardware or process to connect to a Saudi Aramco network or Saudi Aramco Systems.
Risk	The measurement and articulation of the potential adverse impact on the operation of information systems, which is affected by threat occurrences on organizational operations, assets, and people.
Risk Assessment	The overall process of calculating the potential impact of an event using metrics-based risk identification, analysis and evaluation.
Risk Management	The process of recognizing Risk; assessing the impact and likelihood of that Risk; and developing strategies to manage it, such as avoiding the Risk, reducing the negative effect of the Risk and/or transferring the Risk.
Sanitization	The process of permanently removing all data and/or licensed software, through overwriting or degaussing methods, from an Asset before that Asset is disposed, loaned, destroyed, donated, transferred, or surplus.
Sender Policy Framework (SPF)	Email-validation system that allows domain owners to publish a list of authorized IP addresses or subnets to detect and block email spoofing, and reduce the amount of spam, fraud and phishing
Standard	Provides information security requirements that support the implementation of the policy.
Suspicious Activities	Any observed user, system or network traffic behavior that could indicate or lead to a cyberattack on Assets that are used to receive, access, store, process or transmit Saudi Aramco data.
Systems	A collection of communication and computing hardware, software, firmware, database and applications organized to accomplish a specific function or set of functions.
Technology Asset(s)	Any information technology or operational technology system, network, or device that is owned, operated, leased, or controlled by the company or that stores or processes data to include any hardware or software.

Term	Definition
Third Party	Any external party; individual, business or organization that generates, acquires, compiles, transmits or stores data on behalf of Saudi Aramco.
Threat	An activity, event or circumstance with the potential for causing harm to information system resources.
Vulnerability	Any known or unknown deficiency in an information system, application or network that is subject to exploitation or misuse by threat agents.
Vulnerability Assessment	A process that defines, identifies, and classifies the security weaknesses/exposures (Vulnerabilities) in a computer, network, or communications infrastructure in order to apply a patch or fix to prevent a compromise and ensure adherence with the Standard.
Waiver	An exception or exemption to any written information security policy, standard, procedure, or practice that has been approved by the appropriate governing body and published for use.




I. Purpose


Third Party Cybersecurity Standard (TPCS) sets forth the minimum Cybersecurity requirements for Saudi Aramco Third Parties to protect Saudi Aramco from possible cyber threats and strengthen Third Parties' security posture.

II. Scope

This Standard applies to All Third Parties engaging with Saudi Aramco through contractual agreements.

Additional specific cybersecurity requirements are defined for a Third Party whom below classes might describe:



-  • **Network Connectivity:** Third Party computing infrastructure is provided with network connectivity to Saudi Aramco Corporate Network to access Saudi Aramco intranet services and perform required work. This connectivity is provided through leased lines or through certain VPN solutions such as SSL VPN over private links or site-to-site VPN over the Internet.
-  • **Outsourced Infrastructure:** Third Party is managing, maintaining and/or supporting a computing infrastructure on behalf of Saudi Aramco.
- **Critical Data Processor:** Third Party is developing, accessing and/or processing Saudi Aramco Critical Data.
- **Customized Software:** Third Party is developing and/or hosting a customized software, application, website or solution for Saudi Aramco.
-  • **Cloud Computing Service:** Third party is providing Public Cloud Computing service to host, store and/or process Saudi Aramco data. This includes any cloud computing service model; such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

 TPCS aims to effectively protect Assets and Critical Facilities that are accessed, processed, communicated to, or managed by Third Parties through providing the

required Cybersecurity Controls. It is the responsibility of the Third Party to ascertain and meet the requirements of this Standard as applicable.

III. Change Control

Changes made to the Standard documentation will be highlighted using the following labeling scheme.

Status	Name	Description
	Modified	An existing standard or guideline that has been changed.
	New	A new standard or guideline that has been added and approved for this release.

IV. Conflicts and Deviations

In the event compliance with this standard is not technically feasible, a waiver must be requested.

V. Revision

At a minimum, this document will be reviewed, and updated annually or as required, by Saudi Aramco Information Security Department, to ensure that it continues to meet the business requirements. Updates to this Standard will be communicated to the Third Party on an annual basis or where a significant requirement is embedded.

VI. Cybersecurity Controls Instructions



- At a minimum, all Third Parties must comply with all cybersecurity controls specified in Section VII (A) of this Standard.
- Additionally, a Third Party may fall under more than one classification, described above, based on the provided level of accessibility to Assets and Critical Facilities (hereinafter together referred to as “Assets”) as required by the work specified in the Contract. The Third Party that falls under those classes must also ensure adherence with cybersecurity controls specified in Section VII (B) in this Standard.



- Third Party must comply with all cybersecurity controls specified in the appropriate class as communicated by Saudi Aramco. These cybersecurity controls must apply throughout the Data Life Cycle.
- All cybersecurity controls specified in this Standard must be implemented on:
 - All Third Party information systems and/or Assets used to connect to Saudi Aramco's network.
 - All Third Party's Assets hosting, receiving, storing, processing or transmitting Saudi Aramco data. These Assets must be secured and stored in keeping with this Standard and must be made available to authorized users on a need-to-know basis.

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 polices.
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					✓



CNTL No.	Control Name	Network Connectivity	Outsourced Infrastructure	Critical Data Processor	Customized Software	Cloud Computing Service
TPC-29	If Third Party is hosting a website for Saudi Aramco, annual Penetration Testing must be conducted to test website security.				✓	
TPC-30 	Third party data center must be certified by industry recognized authority					✓
Risk Management Strategy (RM)						
TPC-31	Third Party must have a process to conduct Cybersecurity Risk Assessment on regular basis, to identify, assess and remediate Risks to data and information systems.	✓	✓			
PROTECT						
Access Control (AC)						
TPC-32 	Users accessing applications and information systems must be issued unique user logins and passwords. Generic accounts must not be allowed, unless explicitly approved, restricted and controlled.	✓	✓	✓	✓	✓
TPC-33 	User access to the operating system, applications and database must be reviewed on a semiannual basis to determine if accessing personnel still require such access.	✓	✓	✓	✓	✓
TPC-34	All privileged accounts must be limited, justified and reviewed on regular basis.	✓	✓	✓	✓	✓
TPC-35	Remote administrative access from the Internet must not be allowed, unless explicitly approved, restricted and controlled.	✓	✓	✓	✓	
TPC-36 	Network connections to information systems and applications at the Third Parties location must be authorized and monitored.	✓	✓			✓
TPC-37	Multi-factor authentication must be enforced on all privileged accounts access including remote access to information systems and applications.	✓	✓	✓	✓	✓
TPC-38	Third Party must logically (e.g. partitioning a physical drive) and/or physically segregate data-at-rest related to Saudi Aramco from the data of other clients or customers.	✓	✓	✓	✓	✓
TPC-39	Saudi Aramco Critical Data documents must only be shared with limited individuals who are part of the work specified in the Contract.			✓		


CNTL No.	Control Name	Network Connectivity	Outsourced Infrastructure	Critical Data Processor	Customized Software	Cloud Computing Service
TPC-40	Servers and workstations subnets must be segmented and access between them is restricted and monitored.	✓	✓			
TPC-41	Servers accessible from the Internet must be placed in a DMZ (i.e. perimeter network) with restricted access to internal subnets.	✓	✓	✓		
TPC-42	Wireless networks accessing information systems must use strong encryption for authentication and transmission, such as WPA2 or WPA2 Enterprise.	✓	✓	✓	✓	✓
TPC-43 	Third Party data center must have the required tier rating and high-availability of service fail-over as determined by Saudi Aramco					✓
TPC-44 	Multi-Factor authentication must be enforced on Saudi Aramco users accessing Cloud Service Provider's Public Cloud Computing Service storing or hosting Saudi Aramco Critical Data.					✓
TPC-45 	Multi-Factor authentication must be enforced on end-users accessing Content Management Services (CMS) of Cloud Computing Service.					✓
TPC-46	All systems (routers, switches, servers and firewalls) must be housed in a communication room and locked rack(s). The access to the communication room must be contingent on security requirements such as access card readers or biometric devices.	✓	✓	✓	✓	✓
TPC-47 	Third party must define a process for visitor management. The process should include maintaining and regularly reviewing visitor logs. The visitor log should capture information such as: - Visitor identification (e.g. Government ID) - Visit Purpose - Check in/check out date and time	✓	✓	✓		
TPC-48	Visitors accessing Critical Facilities must be escorted at all times.	✓	✓	✓		
TPC-49	Third Party must dedicate an access restricted working area for personnel with access to Saudi Aramco network.	✓				


CNTL No.	Control Name	Network Connectivity	Outsourced Infrastructure	Critical Data Processor	Customized Software	Cloud Computing Service
Data Security (DS)						
TPC-50	Backup media must be secured to block/inhibit unauthorized physical access.	✓	✓	✓	✓	✓
TPC-51	Technology Assets and Systems connected to the internet must be licensed and supported by the provider.	✓	✓			
TPC-52	Third Party must encrypt data in transit (e.g. SSH, FTPS, HTTPS, TLS, IPSEC).		✓	✓	✓	✓
TPC-53 	Third Party must encrypt (e.g. using HTTPS) sessions where Critical Saudi Aramco information or data will be transmitted from and to the Public Cloud Computing Services, and enforce session authentication, lockout, and timeout.					✓
TPC-54	Third Party must implement encryption mechanisms, using at least AES encryption algorithm, and 256 bit key, on all devices or storage media hosting sensitive data per the Third Party's assets classification policy.	✓	✓	✓		✓
TPC-55 	Encryption key management capability, including preservation and retrieval, must be defined, applied, and periodically reviewed.					✓
TPC-56	Third Party must implement a device control mechanism on Assets that are used to receive, store, process or transmit Saudi Aramco data such as disabling the use of external storage media.	✓	✓			✓
TPC-57	Access to the Internet must be restricted by Content-filtering technologies to block: <ul style="list-style-type: none"> • Malicious and suspicious websites. • Personal and non-company email services. • Personal and non-company approved public cloud services. 	✓	✓	✓		
TPC-58	Documents containing Saudi Aramco Critical Data, must be encrypted and stored securely with access limited to authorized personnel.			✓		
TPC-59	Remote wipe solution must be installed on all tablets and mobile phones used to receive,			✓		

CNTL No.	Control Name	Network Connectivity	Outsourced Infrastructure	Critical Data Processor	Customized Software	Cloud Computing Service
	store and/or produce Critical Data for Saudi Aramco.					
TPC-60 	Third Party must implement data validation on all input fields for applications or Cloud Computing Services used by Saudi Aramco to only accept input with valid data type, syntax and length range.				✓	✓
TPC-61 	Application error messages must not display any sensitive technical information.				✓	✓
TPC-62 	Application or Cloud Computing Services must not store, generate, transmit, or use plain-text passwords.				✓	✓
Information Protection Processes and Procedures (IP)						
TPC-63	Third Party must create and manage baseline configurations to harden information systems. The hardening process must address configurations such as: <ul style="list-style-type: none"> Resetting default usernames/passwords Disabling unneeded software Disabling unneeded services Removing administrative access of users on workstations. 	✓	✓	✓	✓	✓
TPC-64	Third Party must establish and follow regular procedures for backup of critical systems and Saudi Aramco's data, software and websites.	✓	✓		✓	✓
TPC-65 	Backup stored at an off-site location must be encrypted using at least AES encryption algorithm, and 256 bit key, except for data classified as public.	✓	✓	✓	✓	✓
TPC-66	Third Party must implement a sanitization process before any Assets are loaned, donated, destroyed, transferred, or surplus. The process must be aligned to industry best practices such as NIST 800-88.	✓	✓	✓	✓	✓
TPC-67	Third Party must have a Disaster Recovery Plan (DR Plan) which is documented, maintained and communicated to appropriate parties. The DR Plan should address the recovery of Assets and communications following a major disruption to business operations.	✓	✓		✓	✓

CNTL No.	Control Name	Network Connectivity	Outsourced Infrastructure	Critical Data Processor	Customized Software	Cloud Computing Service
TPC-68	Third Party must have a comprehensive Business Continuity (BC) plan which is documented, maintained and communicated to appropriate parties. The BC plan should address the occurrence of the following scenarios: a) Equipment failure. b) Disruption of power supply or communication. c) Application failure or corruption of database. d) Human error, sabotage or strike. e) Malicious Software attack. f) Hacking or other Internet attacks. g) Social unrest or terrorist attacks. h) Environmental disasters. i) Emergency contact information for personnel.	✓	✓		✓	✓
TPC-69	Third Party must ensure that owners of the Business Continuity (BC) plan are identified and that the BC plan is reviewed and updated annually.	✓	✓		✓	✓
TPC-70	Third Party must conduct Business Continuity drills at least annually.	✓	✓		✓	
TPC-71 	Third Party must have formal procedures for on-boarding employees. On-boarding procedures must include background checks (e.g. Verification of work histories).	✓	✓	✓	✓	✓
TPC-72 	Third Party must conduct security and source-code vulnerability scanning on all developed applications, and close all discovered vulnerabilities before deployment in production.				✓	
TPC-73	All changes to the application must be properly authorized and tested in a testing environment before moving to production.				✓	
TPC-74 	Third Party must have a process for secure system and software development life cycle in alignment with industry best practice.				✓	✓

CNTL No.	Control Name	Network Connectivity	Outsourced Infrastructure	Critical Data Processor	Customized Software	Cloud Computing Service
Protective Technology (PT)						
TPC-75	Third Party must retain all audit logs from information systems and applications storing, processing or transmitting Saudi Aramco data for one (1) year.	✓	✓		✓	✓
TPC-76	Firewalls must be implemented at the network perimeter and only required services must be allowed. Vulnerable services or insecure protocols should be blocked.	✓	✓	✓	✓	✓
TPC-77	Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) must be implemented at the network perimeter.	✓	✓	✓	✓	✓
TPC-78	Signatures of firewalls, IDS and IPS must be up-to-date.	✓	✓	✓	✓	✓
TPC-79 	If Third Party is hosting an application or a website for Saudi Aramco or providing cloud-based web application, Web Application Firewall (WAF) must be implemented to inspect all incoming traffic for potential threats and malicious activity e.g. SQL injection and Cross Site Scripting.				✓	✓
DETECT						
Anomalies and Events (AE)						
TPC-80	Third Party must monitor Technology Assets, Systems and applications to identify unauthorized access, or unauthorized activity.	✓	✓			✓
TPC-81 	Third Party must periodically aggregate and correlate data from multiple systems and critical applications such as Firewalls, IDS/IPS, and anti-virus in a central repository for event monitoring and analysis purposes.	✓	✓		✓	✓
Continuous Monitoring (CM)						
TPC-82	Multiple physical security measures must be implemented to prevent unauthorized access to facilities. Entrances and exits must be secured with authentication card key, door locks and monitored by video cameras.	✓	✓	✓		

CNTL No.	Control Name	Network Connectivity	Outsourced Infrastructure	Critical Data Processor	Customized Software	Cloud Computing Service
TPC-83	Privileged accounts activity must be logged and monitored on a regular basis.	✓	✓		✓	✓
TPC-84	Non-authorized devices (such as personal devices and mobile phones) must not be used to store, process or access Assets.	✓	✓	✓		
TPC-85	Monthly Vulnerability scans must be conducted to evaluate configuration, Patches and services for known Vulnerabilities.	✓	✓	✓	✓	✓
TPC-86	Physical access to the facility where information systems reside must be restricted to authorized personnel and reviewed on a regular basis.	✓	✓	✓		✓
TPC-87	Information systems and applications must log auditable events as stated in Appendix C.	✓	✓		✓	✓
RESPOND						
Communications (CO)						
TPC-88	Incident management policy and plan must be documented, maintained and communicated to management and appropriate team members.	✓	✓	✓	✓	✓
Analysis (AN)						
TPC-89	Third Party must have an Incident Response capability that includes preparation, detection and analysis, containment, eradication, recovery, documentation and preservation of evidence, communication protocols and lessons learned.	✓	✓		✓	✓
TPC-90	Third Party must track, classify and document all Cybersecurity Incidents.	✓	✓			
Mitigation (MI)						
TPC-91 	Third Party must resolve or mitigate the identified security Vulnerabilities on a system, computer, network, or other computer equipment within the following timeframes: - Critical Risk: immediate correction up to fourteen (14) calendar days of critical vendor	✓	✓	✓	✓	✓

CNTL No.	Control Name	Network Connectivity	Outsourced Infrastructure	Critical Data Processor	Customized Software	Cloud Computing Service
	patch release, notification from Saudi Aramco, or discovered security breach whichever is earlier. - High Risk: within one (1) month of vendor patch release, or discovered security breach whichever is earlier. - Medium and Low Risk: within three (3) months of discovery.					
TPC-92 	If Third Party is hosting a website for Saudi Aramco or providing a Cloud Computing Service, the website / Cloud Computing Service must be secured by a Distributed Denial of Service (DDOS) protection.				✓	✓

VIII. Reference

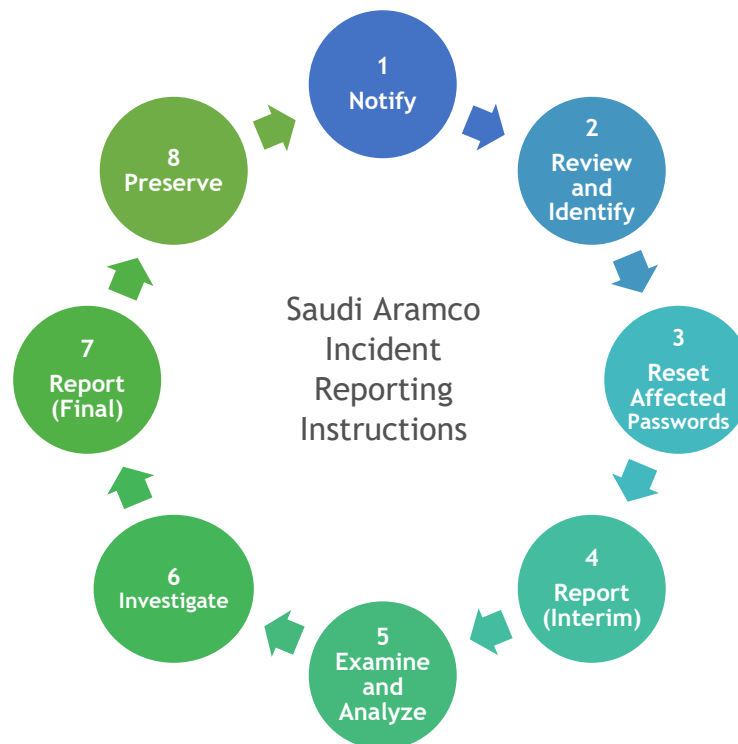
- National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)

IX. Approval



Basim A. Al-Ruwaii
Chief Information Security Officer

Appendix A - Cybersecurity Incident Response Instructions



1. Notify

- Notify Saudi Aramco Security Operations Center (SOC) via the Saudi Aramco Security Hotline at: +966 (13)-880-0000.
- Subsequent notification should be communicated via the communication method agreed by SOC during the initial notification.

2. Review and Identify

- Immediately review all recent changes and modifications to information system users and access privileges for unauthorized modifications.
- Conduct a thorough review of the Third Party's information systems for evidence of compromise.

3. Reset Affected Passwords

- Immediately change every password on information systems that are compromised or suspected to be compromised due to the Incident.

4. Report (Interim)

- Provide Saudi Aramco with reports detailing the Incident. The Third Party must communicate its ongoing efforts to mitigate and resolve the Incident every twenty-four (24) hours until the time of Incident resolution. Please refer to Appendix B.1 for details of the report template. The Incident must be classified according to the below classification:

Severity	Description
Low	Incident that: <ul style="list-style-type: none"> • Adversely impacts a very small number of systems or individuals • Disrupts a very small number of network devices or segments • Has little or no risk of propagation or causes only minimal disruption or damage
Medium	Incident that: <ul style="list-style-type: none"> • Adversely impacts a moderate number of systems and/or people • Adversely impacts a non-critical organization system or service • Adversely impacts a business unit system or service • Disrupts a business unit network
High	Incident that: <ul style="list-style-type: none"> • Threatens to have a significant adverse impact on a large number of systems and/or people • Poses a potential large financial risk or legal liability to the organization • Threatens the confidentiality of data • Adversely impacts an organization system or service critical to the operation of a major portion of Saudi Aramco • Has a high probability of propagating to many systems and causing significant damage or disruption

5. Examine and Analyze

- Upon request by Saudi Aramco, provide access to information or equipment associated with the reported Incident for the purpose of conducting a forensic analysis. This includes but not limited to hard disk drives, volatile memory dumps and logs.

6. Investigate

- Submit (or provide access) to Saudi Aramco SOC, any malicious software/program, supporting binaries and files associated with the Incident for forensic analysis purpose. The suitable submission method will be defined by Saudi Aramco upon receiving the first *Interim Status Report*.

7. Report (Final)

- Provide Saudi Aramco with two Final Reports of the Incident:
 - a. *Business Report:* High-level report for Saudi Aramco Management within three (3) business days of resolution or a determination that the problem cannot be resolved within such time period. Please refer to Appendix B.2-1 for details of the reports template.
 - b. *Technical Report:* detailed report for Saudi Aramco cybersecurity team within ten (10) business days of resolution or a determination that the problem cannot be resolved within such time period. Please refer to Appendix B.2-2 for details of the reports template.

8. Preserve

- Preserve images of all known affected information systems for at least ninety (90) days from the submission of the Final Report.

Appendix B - Cybersecurity Incident Subsequent Reports and Notifications

B-1 Interim Status Reports

The Third Party must provide Saudi Aramco SOC with an interim written status report of each Cybersecurity Incident within 24 hours from initial incident notification. The subsequent Interim Status Reports must be provided to Saudi Aramco SOC every 24 hours until the Cybersecurity Incident is resolved. The following report must be used:

Third Party Cyber Incident Interim Status Report			Report No.: #
Date:	MM/DD/YYYY	Third Party Incident Coordinator Information	
Third Party Name:		Name:	
		Email:	
		Phone/Mobile:	
Incident Classification:			
Incident Description:			
Known/Suspected cause:			
Incident Impact:			
Type of information affected:			
Incident Response Activities			
Actions taken:			
Future actions that will be taken:			
Current incident status:			
Expected timeframe for full service restoration:			

B-2 Final Report

1. Business Report

The Third Party must provide Saudi Aramco SOC with a final written report of any Cybersecurity Incident within three (3) business days of resolution or a determination that the problem cannot be resolved within such time period, such report must include:

- The Third Party's Name
- The Third Party's Incident Coordinator and contact information
- The Saudi Aramco Incident Coordinator
- Date and Time of the Incident
- Incident Classification (according to Saudi Aramco classification provided in this document)
- Length of Outage and Impact (i.e. Reputational, operational, customer, financial and legal).
- Incident Executive Overview

2. Technical Report

The Third Party must provide Saudi Aramco SOC with a final written report of any Cybersecurity Incident within ten (10) business days of resolution or a determination that the problem cannot be resolved within such time period, such report must include:

- The Third Party's Name
- The Third Party's Incident Coordinator and contact information
- The Saudi Aramco Incident Coordinator
- Date and Time of the Incident
- Incident Classification (according to Saudi Aramco classification provided in this document)
- Impact and Length of Outage
- Incident Executive Overview including the Incident impact (i.e. Reputational, operational, customer, financial and legal).
- Incident Details:
 - List of individuals and other Third Parties that were involved with any aspect of the Incident handling
 - How/when the Incident was initially detected
 - How/when the Incident was initially reported to Saudi Aramco

- Description of what resources/services were impacted
- Description of Incident's impact to Saudi Aramco (volume and type where applicable)
- Containment - How was the Incident contained
- Root Cause - What was the cause for disruption
- Corrective action during the Incident - What steps were taken to reduce exposure during the Incident (in most cases, there are interim steps taken to reduce exposure, e.g., Filtering, rerouting services, etc.)
- Permanent corrective actions/preventative measures - What permanent corrective actions have been put in place as a result of this Incident
- Conclusion

Appendix C - Auditing Events

Information Systems must be capable of auditing the events listed below.

No.	Event Type
1	System start
2	System shutdown
3	System restart
4	Successful login attempts (Logon Types must be included)
5	Failed login attempts
6	Service creation
7	Additon of user account
8	Deletion of user account
9	Escalation/modification of account priviliges
10	Modificaiton of security configuration/policies
11	Deletion of user accounts
12	Activities of privileged accounts
13	Logs cleared
14	Attempt/Failure to access removable storage
15	Session connected, reconnected and disconnected
16	Plug and Play driver install attempted (System Log)
17	Encryption keys access

No.	Event Attributes
1	Timestamp
2	User ID
3	Event name
4	Event category
5	Event severity
6	Host name
7	Source IP address
8	Destination IP address
9	Source Port
10	Destination Port

