CONTENT

This General Instruction (GI) outlines the mandatory minimum information security requirements to support the protection of confidentiality, integrity, and availability of Saudi Aramco information and technology assets.

The content of this GI includes:

1. PURPOSE

This Enterprise Cybersecurity Policy sets forth the mandatory minimum information security requirements for protecting, maintaining and continually improving the overall information security posture of Saudi Aramco information and technology assets. The policy is in alignment with INT-7 (Data Protection and Retention) and NIST Cybersecurity Framework (CSF) for Critical Infrastructures.

2. SCOPE

The scope of this Enterprise Cybersecurity policy applies to all Saudi Aramco organizations who have information or systems.

3. DEFINITIONS

3.1 Asset - 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.

3.2 Availability - Timely, reliable access to information and information services for authorized users.

3.3 Baseline Security Configuration - Mandatory minimum security requirements necessary for an information system to enforce the security policy and maintain an acceptable level of risk.

3.4 Business - Any organization within or contractually obligated to Saudi Aramco that utilizes Systems to process their business information.

3.5 Chief Information Security Officer (CISO) Office - Provides independent and comprehensive Information Security Risk Management and delivers guidance and oversight for activities designed to enhance Saudi Aramco's Information Security posture and maturity.

3.6 Confidentiality - The preservation of authorized restrictions on information access and disclosure.

3.7 Countermeasure - Action, device, procedure, mechanism, technique, or other measure that reduces the vulnerability of an information system to unauthorized activity.

3.8 Criticality - A metrics and risk-based measurement of the impact that the failure of the system to function as required will have on the organization.

3.9 Critical Facilities - A physical location housing information processing Systems such as data centers, communications closets, or cabling (power, network etc.).

3.10 Data - A representation of facts, concepts, information, or instructions suitable for communication, processing, or interpretation by people or information systems.

** 3.11 EMSR – Executive Management Safety Reviews

3.12 Enterprise Risk Management (ERM) - An enterprise-wide set of coordinated activities, embedded within strategic and operational policies and practices, whereby an organization manages all of its risks.

3.13 Incident - The actuality or potential likelihood an event or occurrence that jeopardizes the confidentiality, integrity, or availability of Technology Assets or an event that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

3.14 Industrial Control Systems (ICS) - The technological infrastructure supporting industrial processes, including such functions as receiving telemetry, analyzing measurements against established set points, and controlling field devices; examples of ICS include Process Control Systems (PCS), Distributed Control Systems (DCS), Power Automation and Supervisory Control and Data Acquisition (SCADA).

3.15 Integrity - The maintenance and protection of information systems and information from unauthorized modification to ensure the quality, accuracy, completeness, nonrepudiation, and authenticity of information.

** 3.16 KPI – Key Performance Indicator is a measure of performance, commonly used to help define and evaluate how successful it is, typically in terms of making progress towards its long-term organizational goals.

3.17 Least Functionality - Configures the System to provide only required capabilities e.g. prohibits or restricts the use of unneeded functions, ports, protocols, and/or services.

3.18 Mobile Devices - Portable self-contained electronic devices, such as laptops, tablets, cell phones, or mobile cameras whether connected or not to the Saudi Aramco network or other privately held data network.

3.19 Network Segregation - The physical or logical separation of groups of users, information systems or data networks and their related services that aggregate similar business functions by control of network traffic flow, e.g. by use of security gateways, physically separate networks, or access controls.

** 3.20 Performance Review - a regular admin area event to review admin area major initiatives and performance indicators related to cybersecurity.

** 3.21 Phishing Dashboard: Dashboard that contains up-to-date phishing email test results for the corporate.

3.22 Process and Procedure - A series of steps to be followed as a consistent and repetitive approach or cycle to accomplish an end result.

3.23 Remote Access - Act of utilizing a remote access service, hardware or process to connect to a Saudi Aramco network or Saudi Aramco Systems.

3.24 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.

3.25 Risk Appetite - Amount and type of risk, which is understood, and that an organization is willing to accept while maintaining functionality.

3.26 Risk Assessment - The overall process of calculating the potential impact of an event using metrics-based risk identification, analysis and evaluation.

3.27 Risk Tolerance – Organization readiness to bear the risk after risk treatment in order to achieve its objectives.

3.28 Saudi Aramco Engineering Standards (SAES) - establish minimum mandatory requirements for the selection, design, construction, maintenance, and repair of equipment and facilities. The requirements in these standards apply Company-wide.

3.29 Saudi Aramco Engineering Procedures (SAEPs) - establish instructions and responsibilities associated with various engineering activities. This document contains the instructions to initiate, format, prepare, revise, coordinate and obtain approvals for all SAEPs.

SAEPs are procedures, approved by Saudi Aramco Management, that establish minimum requirements for dealing with their associated subject material.

3.30 Security Architecture – Cohesive security design, which addresses the requirements and in particular the risks of a particular environment/scenario, and specifies the required security controls.

3.31 Security Policy - The set of laws, rules, directives and practices that governs how an organization protects information systems and information.

3.32 Segregation of Duties – An internal control that prevents or detects errors and irregularities by assigning to separate individuals the responsibility for initiating and recording transactions and for the custody of assets.

3.33 Standard – Provides information security requirements that support the implementation of this policy.

3.34 Supply Chain - Supply chain consists of organizations that design, produce, source, and deliver products and services to Saudi Aramco.

3.35 Support Entities – An organization that supports the operations of processing, storing or safeguarding data on behalf of the business.

3.36 System - A collection of communication and computing hardware, software, firmware, and applications organized to accomplish a specific function or set of functions.

3.37 Technical Controls – Security controls executed by the computer system through mechanisms contained in the hardware, software and firmware components of the system.

3.38 Third Party – Any external party; individual, business or organization that generates, acquires, compiles, transmits or stores data on behalf of Saudi Aramco.

3.39 Threat - An activity, event or circumstance with the potential for causing harm to information system resources.

** 3.40 Training Management System (TMS): System enables employee to access training program.

3.41 Vulnerability – Any known or unknown deficiency in an information system, application or network that is subject to exploitation or misuse by threat agents.

4. ACCOUNTABILITY, RESPONSIBILITY AND DELEGATION

The CISO Office is the sole accountable and responsible entity for all information security oversight functions corporate-wide, including governance, risk management and compliance management (GRC). Business organizations are accountable and responsible for all information security operational functions of their information and information systems. These responsibility may be delegated to Support Entities, however, the business organizations are ultimately accountable for their information and information systems.

This policy is written based on the current model and structure of Support Entities (Security Operations), which is a de-centralized model. The policy is subject to change based on a new structure or model, for example a centralized entity for Security Operations.

5. GOVERNING AND AUTHORITATIVE DOCUMENTS

In order to meet the policy requirements and mitigate relevant risks, responsible entities are expected to develop and maintain standard and procedure documents, based on recognized industry best practices suitable for their business environments. The following are the only recognized information security governing document types with their mandated lifecycle. These document types are ordered by precedence level. In case of any conflict, higher level governing document types shall supersede.

Document Type	Owner	Approver	Format	Minimum Review Cycle
Directions	Management Committee	CEO	INT	Every 5 years
Policies	CISO Office	CISO	GI	Every 3 years
Standards	Business Organizations	Engineering Committee/Proponent Manager	SAES	Annual
Processes/Procedures	Business Organizations	Engineering Committee/Proponent Manager	SAEP	Annual

Cybersecurity Standards:

5.1. Cybersecurity standards must conform to the mandatory minimum requirements of this Enterprise Cybersecurity Policy.

5.2. Cybersecurity standards must be developed, maintained and communicated by Business Organizations.

5.3. Cybersecurity standards must be reviewed by the CISO office

5.4. Cybersecurity standards must be approved by Engineering Committee/Proponent Manager

5.5. Cybersecurity standards must be reviewed whenever there is a major change in the environment, or at least every year.

5.6. Cybersecurity standards must be aligned with best practices.

5.7. Cybersecurity standards must be SMART (Specific, Measurable, Attainable, Realistic, and Timely).

Process and Procedures:

5.8. Process and procedures must conform to cybersecurity standards.

5.9. Process and procedures must be developed, maintained and communicated by Business Organizations.

5.10. RACI (Responsible, Accountable, Consulted and Informed) must be developed and maintained within the process and procedures document.

5.11. Information security process and procedures must be approved by Engineering Committee/Proponent Manager

5.12. Process and procedures must be reviewed whenever there is a major change in the environment, or at least every year.

6. SUPPORTING DOCUMENT

Baseline Security Configuration and Design Documentation:

6.1. Baseline security configuration and design documentation must conform to the mandatory minimum requirements of the cybersecurity standards.

6.2. Baseline security configuration and design documentation must be developed, maintained and communicated by the Proponent Manager.

6.3. Baseline security configuration and design documentation must be approved by at least the division head of the respective organization.

6.4. Baseline security configuration and design documentation must be reviewed whenever there is a major change in the environment, or at least every year.

7. POLICY:

7.1. CISO

The CIOS Office is the centralized entity that provides independent, unified and comprehensive Information Security Governance, Risk & Compliance (GRC) management and establishes guidance & oversight for activities to enhance Saudi Aramco's information security posture. The following are mandatory minimum cybersecurity requirements that the CISO office is accountable for implementation.

7.1.1. Information Security Governance

7.1.1.1. Corporate information security strategy must be developed, maintained and communicated.

7.1.1.2. Enterprise Cybersecurity Policy must be developed, maintained and communicated.

7.1.1.3. Enterprise Cybersecurity Policy must comply with Saudi Arabia's law and regulation.

7.1.1.4. Information security maturity and posture must be reported to corporate management.

7.1.1.5. Information security awareness material must be developed to maintain ongoing education for End-users.

7.1.1.6. Information security behavior management strategy and road map must be developed, maintained and communicated to respective stakeholders.

7.1.1.7. Specialized training must be provided to corporate and executive management regarding their information security role and responsibilities.

7.1.1.8. Oversight Information Security Architecture must be developed, maintained and communicated.

7.1.2. Information Security Risk Management

7.1.2.1. Information security risk management framework must be established, managed, approved and aligned with Enterprise Risk Management.

7.1.2.2. Information security Risk Tolerance must be aligned with Enterprise Risk Management (ERM) taking into consideration the business role in critical infrastructure and sector specific risk analysis.

7.1.2.3. Information security risk management must be reported to corporate management on a regular basis based on ERM's criteria.

7.1.3. Information Security Compliance

7.1.3.1. Information security compliance assessment must assess whether information security functional and technical controls are implemented and operating effectively in accordance with approved information security policies and supporting documents.

7.1.3.2. Information security compliance assessment against Third Parties must be conducted to ensure that information security is consistently implemented and operating effectively in accordance with approved information security policies and supporting documents.

7.1.3.3. Information security compliance assessment must use multiple forms of security testing to validate the effectiveness of the implemented controls.

7.1.3.4. Information security compliance must be reported to corporate management on a regular basis.

7.2. Business:

Any organization that utilizes Systems to store, process or transmit Saudi Aramco business information will be required to acquire and/or commit the resources necessary to implement all items provided below. The organizations may delegate some or all of the responsibilities for implementing these requirements to an approved Support Entity. However, the organization is ultimately accountable for the implementation of these requirements. Prior to delegating the responsibility the organization must comply with all requirements of the Support Entity.

7.2.1. General Cybersecurity Requirements

7.2.1.1. Information security initiatives must be aligned with the published Information Security Departments strategy.

7.2.1.2. Information security processes (listed in the subsequent sections) must be defined, measured and continually improved based on industry standards.

7.2.1.3. Roles and Responsibilities (listed in the subsequent sections) for information security processes must be developed, approved by and communicated to appropriate stakeholders.

7.2.1.4. Performance metrics regarding Information security processes (listed in the subsequent sections) must be routinely shared with the CISO.

7.2.2. Asset Management

7.2.2.1. Physical devices and Systems within the organization must be inventoried.

7.2.2.2. Software platform and applications; including specific versioning, dependencies and pre-requisites and third-party contracts, within the organization must be inventoried.

7.2.2.3. Organizational communication and data flows, including to and from third parties must be documented and continually evaluated for risks.

7.2.2.4. External Systems, including those provided or managed by third parties, must be catalogued.

7.2.2.5. Assets must be prioritized based on their classification and Criticality.

7.2.3. Business Environment

7.2.3.1. The organization's role in the Supply Chain must be identified and communicated to respective stakeholders.

7.2.3.2. Dependencies and critical functions for delivery of critical services must be established, continually evaluated and thoroughly documented.

7.2.3.3. Business continuity and resilience requirements against the disruption of critical services must be established, evaluated at least yearly and thoroughly documented.

7.2.4. Information Security Risk Assessment

7.2.4.1. All Assets must be continually assessed for vulnerabilities.

7.2.4.2. Threats and Vulnerability information related to Assets must be received from trusted sources.

7.2.4.3. Internal and external threats must be identified, evaluated and thoroughly documented through a repeatable process.

7.2.4.4. Potential likelihood and impact to the organization must be identified.

7.2.4.5. Risk must be determined based on Threats (internal and external), and Vulnerabilities; likelihoods of occurrence and the potential impact to the organization.

7.2.4.6. Risk responses (accept, mitigate, avoid and transfer) must be thoroughly defined and documented and prioritized.

7.2.4.7. Information security risks must be immediately reported to the Information Security upon their identification.

7.2.5. Information Security Design

7.2.5.1. Security Design process must be established, documented and aligned with CISO Architecture process.

7.2.5.2. Security Design must be aligned with the principle of defense-in-depth that is developed by CISO to protect the confidentiality, integrity and availability of Assets.

7.2.6. Access Control

7.2.6.1. Identities and credentials must be managed for authorized devices and users.

7.2.6.2. Routine and regular evaluation of credentials and levels of access to systems and information must be reviewed at least yearly.

7.2.6.3. Physical access to Assets must be categorized based on risk, managed and protected.

7.2.6.4. Remote Access to Systems must be limited to a quantifiable need, approved by organizational management and routinely evaluated (Remote Access to ICS/SCADA systems or systems involved in the management of critical infrastructure is not permitted).

7.2.6.5. Access to information and Systems must incorporate the principles of least privilege and separation of duties.

7.2.6.6. Network segmentation must be implemented to control the flow of information between interconnected Systems and networks.

7.2.7. Awareness and Training

7.2.7.1. Organizations must communicate information security awareness material to their End-users on a regular basis.

7.2.7.2. Specialized training must be provided to privileged users regarding their information security role and responsibilities.

7.2.7.3. Specialized training must be provided to Third Party stakeholders regarding their information security roles and responsibilities.

7.2.7.4. Specialized training must be provided to physical security personnel regarding their information security role and responsibilities.

7.2.8. Data Security

7.2.8.1. Data-at-rest must be protected using the minimum mandatory requirements.

7.2.8.2. Data-in-transit must be protected using the minimum mandatory requirements.

7.2.8.3. Information Assets must be formally managed through classification, removal, transfer, retention and secure disposal.

7.2.8.4. Data must be hosted on robust, reliable Systems and supported by alternative or duplicate facilities to ensure critical business processes are available when required.

7.2.8.5. Data leakage protection mechanisms must be implemented to prevent unauthorized disclosure of information.

7.2.8.6. Integrity protection mechanisms for information, software and firmware must be implemented to verify integrity is maintained.

7.2.8.7. Development, test and operational environment(s) must be separated to protect against unauthorized access or changes to the operational environment.

7.2.9. Information Protection Processes and Procedures

7.2.9.1. System development life cycle must utilize an approved structured methodology to ensure that security controls are implemented at all stages.

7.2.9.2. Change management process must be implemented to ensure changes to Systems are for valid business reasons, receive proper authorization and do not compromise the security of the System.

7.2.9.3. Backups of information and Systems must be conducted, maintained, and tested at least yearly using proven methodologies.

7.2.9.4. Environmental requirements for physical facilities must be met.

7.2.9.5. Data, media and printed material must be disposed securely in adherence to the classification of the data.

7.2.9.6. Effectiveness of protection technologies must be shared with appropriate stakeholders at regular intervals.

7.2.9.7. Response (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) must be in documented, managed and communicated to stakeholders.

7.2.9.8. Response and recovery plans must be tested at least yearly.

7.2.9.9. Information security must be incorporated in personnel activities including but not limited to provisioning, de-provisioning and screening applicants.

7.2.9.10. Vulnerability management program must be developed, thoroughly documented and maintained.

7.2.10. Maintenance

7.2.10.1. Maintenance, upgrades or repair of Systems must be performed, logged and approved by respective parties using approved maintenance/change management process.

7.2.10.2. Remote maintenance of organizational Assets must be preapproved, logged, and performed to prevent unauthorized access (Remote Access to ICS/SCADA systems or systems involved in the management of critical infrastructure is not permitted).

7.2.10.3. Changes to the organizational structure, business processes, and information processing facilities that affect information security must be documented, preapproved, and communicated to appropriate stakeholders.

7.2.11. Protective Technology

7.2.11.1. Audit logs must be identified, documented, implemented, collected, analyzed, and protected against unauthorized access.

7.2.11.2. Removable computer media must be protected from unauthorized disclosure and in accordance with the classification protection requirements of the information.

7.2.11.3. Access to Systems must be controlled, incorporating the principle of Least Privilege and Functionality.

7.2.11.4. Intrusion Detection/Prevention systems (sensors) must be implemented, configured and monitored to identify security events.

7.2.12. Anomalies and Events

7.2.12.1. Baseline of network operations and systems behavior must be established, and understood to detect deviations from normal operations.

7.2.12.2. Security events must be regularly analyzed to help in the identification of attack vectors, targets, and threats.

7.2.12.3. Security events must be aggregated and correlated from multiple sensors to detect information security events.

7.2.12.4. Security events must be analyzed to determine their impact on the respective organizations. Information collected and lessons learned must be communicated to Information Security to be incorporated into future risk remediation efforts.

7.2.12.5. Incident alert thresholds specific to each system or platform must be established, and implemented to identify potential information security events or malicious activity.

7.2.13. Security Continuous Monitoring

7.2.13.1. Systems processes, network traffic and account activity must be continuously monitored to detect information security events.

7.2.13.2. Critical facilities must be monitored to detect accidents, attacks or unauthorized access.

7.2.13.3. Personnel activity include but not limited to system and data access, must be monitored to detect information security events.

7.2.13.4. Processes used to detect malicious code must be developed and tested at regular intervals.

7.2.13.5. Controls must identify the introduction of unauthorized/malicious code in the environment.

7.2.13.6. Third Party accessing or utilizing the organizations Systems must be monitored to detect information security events.

7.2.13.7. Systems must be monitored for unauthorized personnel, connections, devices, or software.

7.2.13.8. Vulnerability assessments must be performed at regular intervals to identify System vulnerabilities, findings must be communicated to the appropriate stakeholders for remediation.

7.2.14. Detection Process

7.2.14.1. Detection activities must comply with all applicable requirements such as threat cases.

7.2.14.2. Detection processes must be continually reviewed, and tested.

7.2.14.3. Event detection information must be communicated to appropriate stakeholders.

7.2.15. Response Planning

7.2.15.1. The response plan must be executed during or after a declared event.

7.2.16. Response Communication

7.2.16.1. Response personnel must be identified and understand their roles, responsibilities and actions required when a response is needed.

7.2.16.2. Response personnel must be routinely trained consistent with industry best practices.

7.2.16.3. Security events must be reported based on established and approved criteria.

7.2.16.4. Information must be shared consistent with approved response plans.

7.2.16.5. Coordination with stakeholders must occur according to approved response plans.

7.2.16.6. Information shared with external stakeholders to achieve broader information security situational awareness stakeholders must be approved by public relations.

7.2.17. Response Analysis

7.2.17.1. Notifications from detection systems must be investigated.

7.2.17.2. The impact of an incident on the organization must be understood.

7.2.17.3. Forensics activities must be performed.

7.2.17.4. Incidents must be categorized and documented based on the approved response plan.

7.2.18. Response Mitigation

7.2.18.1. Incidents must be contained to limit the damage to the organization.

7.2.18.2. Once an incident has been contained, mitigation steps must be performed.

7.2.18.3. Newly identified vulnerabilities must be mitigated, if the vulnerabilities cannot be mitigated they must be documented and the appropriate countermeasures taken.

7.2.19. Response Improvements

7.2.19.1. Response plans must incorporate lessons learned from ongoing incident handling activities.

7.2.19.2. Response strategies must be updated at least every two years to reduce the likelihood or impact of future incidents.

7.2.20. Recover Planning

7.2.20.1. Recovery plan must be executed during or after an event.

7.2.21. Recover Improvements

7.2.21.1. Recovery plans must incorporate lessons learned from ongoing incidents and process testing.

7.2.21.2. Recovery strategies must be updated at least every two years.

7.2.22. Recover Communication

7.2.22.1. Post-response activities must include public relations involvement.

7.2.22.2. Reputation of the organization post-incident must be repaired.

7.2.22.3. Recovery activities must be communicated to internal stakeholders and management teams in the organization.

** **7.2.23. Reporting Cybersecurity Indicators**

7.2.23.1. Collect all required indicators that are listed in (Supplement I) through the provided solutions such as the Phishing dashboard and TMS following the process in (Supplement II).

7.2.23.2. Communicate Cybersecurity indicators that are listed in (Supplement I) and related to their entity during their EMSR event under the title of (Cybersecurity Indicators)

7.2.23.3. Communicate Cybersecurity indicators that are listed in (Supplement I) and related to their entity during their Performance Review/Dialog

8. EXCEPTIONS

Where compliance is not technically feasible or justified by business needs, an exemption must be submitted in the form of compensating controls and concurred to by Information Security. Business management must accept the risk associated with the exception and concur the compensating control is the only option available. The exemption and compensating control will be reviewed to identify if the exemption is still required and whether the compensating control is effective in minimizing the risk.

9. REVISION

This policy is subject to continuous, systematic review and improvement. It shall be reviewed and updated at least every five years to reflect changes in business objectives and/or risk environment.

10. REFERENCES

- National Institute of Standards and Technology Critical Infrastructure - Cybersecurity Framework (CSF)
- ISO/IEC 27001:2013 Information technology— Security techniques — Information security management systems — Requirements
- NIST 800-53 rev4.
- Data Protection and Retention Policy (INT-7)
- Enterprise Risk Management (INT-13)
- Classification And Handling Of Sensitive Information (GI710.002)
- Sanitization and Disposal of Saudi Aramco Electronic Storage Devices and Obsolete/Unneeded Software (GI299.120)
- General Instructions (GI0.001)

11. APPROVAL

Approval:

Chief Information Security Officer

**12. SUPPLEMENT I - INDICATORS

1. **Phishing KPIs:**

   a. ***Positive*:** number of users who did not click on a link or downloaded an attachment and reported the Phishing email to spam.

   $$\textbf{\textit{Positive}} = \frac{\text{number of users who reported the Phishing email to spam}}{\text{Total number of users who received the test}} \times 100$$

   Organization target must be *100%*

   b. ***Negative:*** number of users who clicked on link or downloaded attachment.

   $$\textbf{\textit{Negative}} = \frac{\text{number of users who clicked on link or downloaded attachment}}{\text{Total number of users who received the test}} \times 100$$

   Organization target must be 0%

   c. ***Neutral:*** number of users who did not click on a link or downloaded an attachment but did not report the phishing e-mail to spam.

   $$\textbf{\textit{Neutral}} = \frac{\text{number of users who have not taken any action or deleted the the phishing email}}{\text{Total number of users who received the test}} \times 100$$

2. **Phishing e-Learning Course:** this KPI is determined based on the users who have failed the phishing test. In order to align with the Consequence management GI, all phishing test failures must take the phishing e-Learning course.

   $$\textbf{Phishing e-Learning Course} = \frac{\text{Number of users who took the Phishing e-Learning course(from the users who failed the test)}}{\text{Total number of users who failed the test}}$$

   Organization target must be 100%

3. **Information Security Essentials e-Learning Course:** All users must take the Information Security Essentials e-Learning course once a year.

   $$\textbf{Information Security Essentials e-Learning Course} = \frac{\text{Number of users who compelted Information Security Essentials e-Learning Course}}{\text{Total number active users}}$$

   Organization target must be 100%

4. **Removable Media Restriction Exceptions waived:** the number of users who are given a waiver to access personal USBs in company workstations/laptops.

$$\textbf{Removable Media Restriction Exceptions} = \frac{\text{Number of users with waivers to access USB's}}{\text{Total number of all users who has netowrk access}}$$

Organization target must be less than or equal 5%

5. **Data Protection Program:** This indicator determines the number of departments that completed the implementation of DPP, departments who are in process of completing the DPP and the Departments that have not yet started the DPP.

Implemented Data Protection Program ***=number of organizations that have Implemented the DPP program***

In progress Data Protection Program ***=number of organizations in the process of completing the DPP program***

Not Started Data Protection Program ***=number of organizations that have not started the DPP program***

Organization target must be 100%

6. **ISA Program KPI:** This indicator determines the number of organizations that acquire and certify ISA(s).
Definition: This KPI determines organizations, which only report directly to GM level or above, supported by ISA(s) and the number of certified ISA(s) that have completed the required certification courses in these organizations.

$$\textbf{Organization supported by ISA} = \frac{\text{Number of orgnizations supportd by full time ISA}}{\text{Total number of orgnizations}} \times 100$$

$$\textbf{Certified ISA(s)} = \frac{\text{Number of certified full time ISA(s)}}{\text{Total number of full time ISAs}} \times 100$$

Organization target must be 100%

7. **Plant Compliance Index:** compliance level of a plant against the approved information security standards.

$$\textbf{Plant Compliance Index} = \frac{Number\ of\ implemented\ security\ controls}{\text{Total number of required controls within the approved information security standards}}$$

This KPI must be reported by July 2017.

8. **Organization Security Maturity Level:** ability of the organization to use the tools/systems and the value the process gives the organizations.

$$\textbf{Organization Security Maturity Level} = \frac{\sum Assessed\ Subcategories\ \ (value\ from\ 0\ to\ 5)}{Number\ of\ Assessed\ Subcategories}$$

Organization should have a target to reach level 4.
This KPI is for the organization that manages computing and communication systems such as IT, ECC and ISO.

** 13. SUPPLEMENT II - PROCESS FOR OBTAINING DATA

1. **Phishing Test Results KPI**

The Information Security Analyst (ISA) of each organization is able & responsible to generate the monthly phishing test email results where he/she can monitor the behavior demonstrated towards the phishing test email including those who repeatedly failed.

The phishing test email result can be generated from the ISA Dashboard.

2. **Data Protection Program KPI**

The Information Security Analyst (ISA) of each organization can approach Data Protection Management Group under (Information Protection Department/Access Management Division) that manage and oversee the Data Protection Program implementation across Saudi Aramco organizations. Data Protection Management Group is able to provide implementation status presenting each organization and namely by those that completed, In-Progress, and Not-Started.

For obtaining the required information, please send an email to (*DPP Review Committee).

3. **Removable Media Restriction Exceptions KPI**

The Information Security Analyst (ISA) of each organization can submit a request to Access Control Solutions Group under (Information Protection Department/Access Management Division) that manage the Active Directory. Access Control Solutions Group is able to provide a detailed report for each organization presenting individuals who has an access.

Detailed report can be requested through CRM > IT Services > Active Directory Management

4. **ISA Program KPI**

The Information Security Analyst (ISA) of each organization can approach Computer Security Administration Group under (Corporate Security Services Division) that oversee and manage the Information Security Analyst Program (ISA) company-wide. Corporate Security Services Division is able to provide the ISA resourcing and certification KPIs.

5. **E-Learning Courses KPI**

The Training Coordinator of each organization can use SAP access role to generate the required eLearning courses results demonstrating those who completed, passed, or failed the subjected eLearning course through Training Dashboard where it's located under MyHome.

For obtaining the required information, please send an email to (*O&BS/S&IS/CSSD/Cmptr Security Admin Group <OG_30001766@Exchange.Aramco.com.sa>).