CONTENT

This General Instruction (GI) outlines the corrective action policy for the failure or violation of Saudi Aramco cybersecurity policies by End Users.

The content of this GI includes:

* 1. PURPOSE

This GI outlines the consequences of negative behavior during planned phishing tests or violations resulting in damage, downtime or inoperability of Saudi Aramco electronic data, network and computing resources.

2. SCOPE

This policy applies to all Saudi Aramco employees and Third-Parties that utilize or have access to Saudi Aramco Technology Assets.

3. DEFINITIONS

The following definitions are specific to this GI:

3.1 End User – means an individual (employee, contractor, or visitor) or a system authorized to access Saudi Aramco's information, computing devices and network resources.

3.2 Incident – means an event or occurrence that actually or potentially jeopardizes the confidentiality, integrity, and 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.

3.3 Information Security Analyst (ISA) – means an individual who is designated within his/her respective organization to implement and enforce data protection programs and is the single point of contact for any information security related activities.

* 3.4 Negative Behavior: Clicking on a link, opening/downloading an attachment in a test phishing email or forwarding the phishing email to other users without meticulously verifying the source and security of the information.

** 3.5 Neutral Behavior: User ignoring the email or simply deleting it from the inbox.

3.6 Systems – means computing and communication software and hardware that are owned or leased by Saudi Aramco.

3.7 Technology Asset – means tangible or intangible property that has value to Saudi Aramco which includes but not limited to information, data, personnel, devices, systems, hardware, software, services and facilities that enable the organization to achieve its business objectives.

3.8 Third-Party – means a person, group or company such as vendor, partner or consultant who supplies product or services to Saudi Aramco.

4. POLICY

Saudi Aramco implemented information security controls to minimize undesirable events that impact employee safety, achievement of business goals, the environment and reliability of operations. These requirements are in place to protect the End Users and Saudi Aramco. Inappropriate use exposes the End Users and Saudi Aramco to risks such as virus attacks, data leakage, compromise or disruption of network systems and services and negative publicity. Securing Saudi Aramco's information and Technology Assets is the responsibility of everyone. Penalties will be imposed on End Users, if they fail to comply with the requirements of Saudi Aramco cybersecurity policies.

4.1. Information Security requirements

4.1.1. Department heads must adopt (such as Data Protection Program developed by IT) or establish an information security program aligned with Saudi Aramco cybersecurity policies including but not limited to Information Security Acceptable Use Policy (GI 299.225).

4.1.2. Department heads must approve, communicate and maintain the information security program to End Users.

4.1.3. Department heads must ensure that information security is integrated and discussed during orientation sessions and department meetings.

4.1.4. Department heads must ensure that specialized training is provided to employees and Third-Party employees regarding their information security roles and responsibilities.

4.1.5. End Users must understand their roles and responsibilities and comply with Saudi Aramco cybersecurity policies.

4.2. Corrective Action and Guidance

4.2.1. Actual Cybersecurity Incident by Employees or Third-Party:

Intentional and unintentional disregard for confidentiality, for personal use or gain or malicious intent or failure to comply with information security safeguards may potentially result in loss of availability, integrity, and confidentiality of systems or data. In the event of an actual cybersecurity incident the following procedures will be followed for corrective action:

4.2.1.1. Thorough review of the case including an approved security report by Corporate Security Services Division and associated End User statements are required to determine if the case is actual.

4.2.1.2. The General Internal Rules for the Organization of Work and Workmen must be used as a basis for determining appropriate disciplinary action for Saudi Aramco employees only.

4.2.1.3. The type of the corrective action must depend upon the facts of the individual case and the Company will consider all relevant factors including the following:

a) The employee/Third-Party intentions when committing the violation that caused the incident.
b) Whether the employee/Third-Party knew that he/she was acting in violation.
c) Whether the employee/Third-Party has been disciplined previously for other violations.
d) If the employee acted dishonestly or with bad intent or was open and transparent in his/her actions.
e) Whether the employee/Third-Party conduct was criminal or malicious.
f) The employee/Third-Party willingness to assist in managing the consequences of the incident, including full cooperation with any subsequent investigation.
g) The severity of the violation and incident.

4.2.2. Negative Behavior

Saudi Aramco reserves the right to assess employees' information security awareness and behavior by using phishing assessment. Saudi Aramco requires employees to exercise a high degree of personal responsibility, sound judgment and common sense while using computing and communicating systems to access its data and information. Hence, End Users must take any assessments seriously to assess and mitigate overall cybersecurity risk.

The failures and their associated corrective actions are as follows:
Employee:

* 4.2.2.1. If an employee fails a phishing test for **the first time** he/she must take an online information security course within 7 working days from the failure. End User, ISA and Group Leader will be notified about the failure.

* 4.2.2.2. If an employee fails **two consecutive phishing tests** within a 12-month (Gregorian) period, the End Users account will be suspended for a maximum period of **1 week**, the account may be activated earlier by an official request from the End User's manager. The End User must retake the online information security course within 7 working days from the account activation and his/her direct supervisor must conduct and document counseling session with the employee. End User, ISA, Group Leader, Division Head and Department Head will be notified about the failure.

* 4.2.2.3. If an employee fails **three consecutive phishing tests** within a 12-month (Gregorian) period; the End user's account will be suspended for a maximum period of **2 weeks**, the account may be activated earlier by an official request from the End user's manager. The End User must retake the online information security course within 7 working days from the account activation and his/her direct supervisor must conduct and document counseling session with the employee. The third consecutive failure will impact the End User's PMP cybersecurity competency rating (please refer to the "Ratings-in-Action" in Supplement II in this GI for further guidelines). End User, ISA, Group Leader, Division Head, Department Head and Admin Area Head will be notified about the failure.

* 4.2.2.4. If an employee fails **four consecutive phishing tests** within a 12 month (Gregorian) period; the End User's account will be suspended for a maximum period of **3 weeks**, the account may be activated earlier by an official request from the End User's manager. The End User must retake the online information security course within 7 working days from the account activation and his/her direct supervisor must conduct and document counseling session with the employee. The fourth consecutive failure will impact the End User's PMP cybersecurity competency rating, please refer to the "Ratings-in-Action" in Supplement II in this GI for further guidelines. End User, ISA, Group Leader, Division Head, Department Head and Admin Area Head will be notified about the failure.

4.2.2.5. If an employee fails **five consecutive phishing tests** within a 12 month (Gregorian) period; the End User's account must be suspended pending the results on an investigation by Corporate Security. The End User's account will only be activated once the investigation by Corporate Security is completed. The employee's PMP cybersecurity competency will be impacted, please refer to the "Ratings-in-Action" in Supplement II in this GI for further guidelines. End User, ISA, Group Leader, Division Head, Department Head and Admin Area Head will be notified about the failure.

Third-Party Employee:

4.2.2.6. If a Third-Party fails an assessment for **the first time** he/she must take an online information security course. The Third-Party, ISA, Group Leader, and Division Head will be notified about the failure.

* 4.2.2.7. If a Third-Party fails **two consecutive phishing tests** within a 12 month (Gregorian) period; his/her account will be suspended for a maximum period of **1 week**, the account may be activated earlier by an official request from the Third-Party Saudi Aramco department manager or above. The End User must retake the online information security course within 7 working days from the account activation and his/her direct supervisor must conduct and document counseling session with the employee. Third-Party, ISA, Group Leader, Division Head and Department Head will be notified about the failure.

4.2.2.8. If a Third-Party fails **three consecutive phishing tests** within a 12 month (Gregorian) period; their account will be suspended for a maximum period of **2 weeks**, the account may be activated earlier by an official request from the Third-Party Saudi Aramco department manager or above. The Third-Party must retake the online information security course within 7 working days from the account activation and his/her direct supervisor must conduct and document counseling session with the Third-Party employee. A notification must be sent to the contract representative notifying them that the Third-Party has failed the assessment three consecutive times within a 12 (Gregorian) month period, this may lead to the separation of the Third-Party employee from the respective contract. Third-Party, ISA, Group Leader, Division Head, Department Head, Admin Area Head and contract representative will be notified about the failure.

4.2.2.9. If a Third-Party fails **four consecutive phishing tests** within a 12 month (Gregorian) period; their account will be suspended for a maximum period of **3 weeks**, the account may be activated earlier by an official request from the Third-Party Saudi Aramco department manager or above. The Third-Party must retake the online information security course within 7 working days from the account activation and his/her direct supervisor must conduct and document counseling session with the Third-Party employee. A notification must be sent to the contract representative notifying them that the Third-Party has failed the assessment four consecutive times within a 12 (Gregorian) month period, this may lead to the separation of the Third-Party employee from the respective contract. Third-Party, ISA, Group Leader, Division Head, Department Head, Admin Area Head and contract representative will be notified about the failure.

4.2.2.10. If a Third-Party fails **five consecutive phishing tests** within a 12 month (Gregorian) period; the Third-Party account must be **suspended** pending the results of an investigation by Corporate Security. Depending on the results of the investigation, the contract representative may be asked to replace the Third-Party resource assigned to the contract. Third-Party, ISA, Group leader, Division Head, Department Head, Admin Area Head and contract representative will be notified about the failure.

5. REFERENCE

- Saudi Arabian Anti-Cyber Crime Law – www.citc.gov.sa
- Saudi Arabian Labor Law.
- Industrial Relations (IR) Manual, Chapter 10.
- General Internal Rules for the Organization of Work and Workmen Internal Work Rules (IWR), Part VI.
- Information Security Acceptable Use Policy GI 299.225

6. APPROVALS

Concur:

_____
CISO, Information Security Department (ISD)

Concur:

_____
Executive Director, Human Resources (HR)

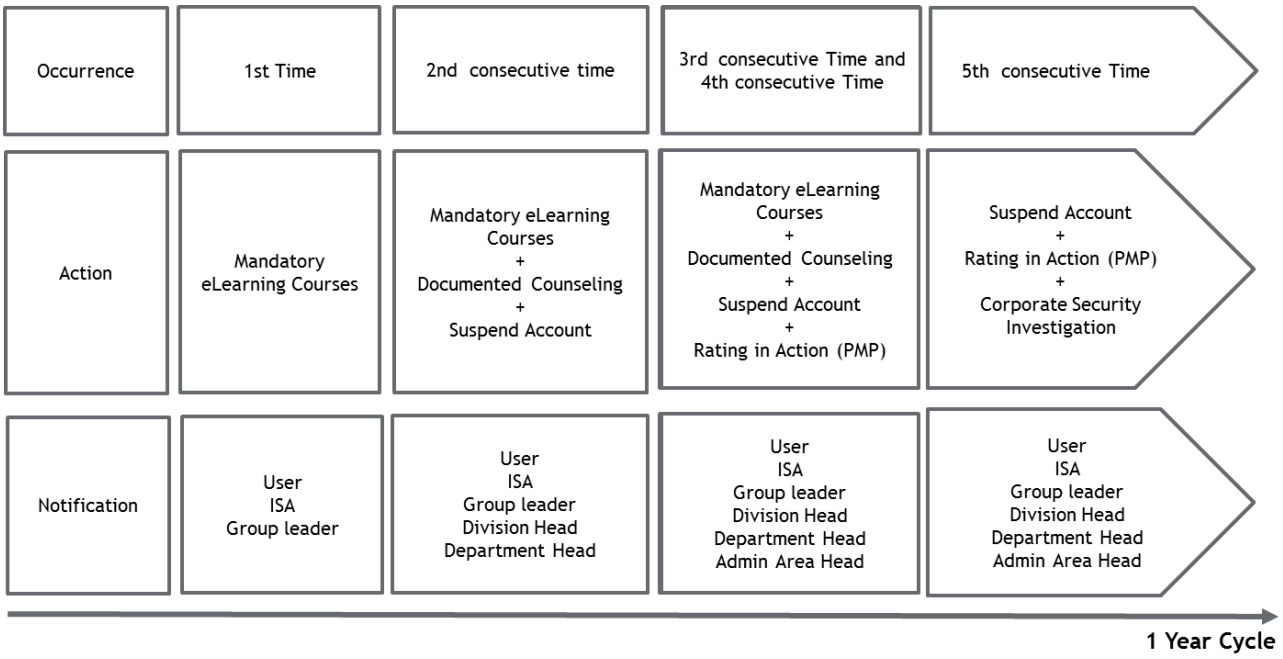
Approval:

_____
Executive Director, Information Technology (IT)

7. SUPPLEMENT I

Negative Behavior

Employee:



Corrective Actions :

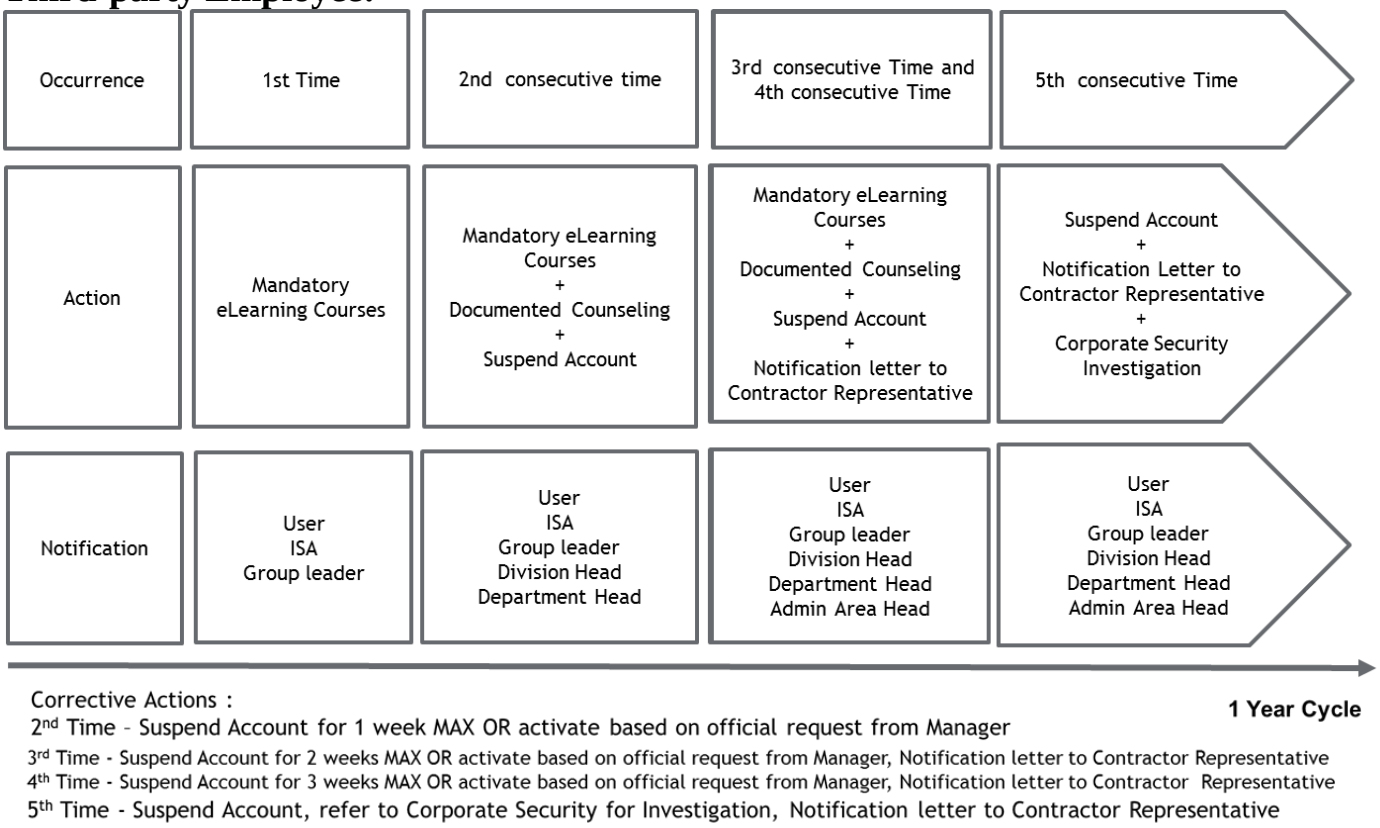
2nd Time - Suspend Account for 1 week MAX OR activate based on official request from Manager

3rd Time - Suspend Account for 2 weeks MAX OR activate based on official request from Manager, Impact PMP refer to Rating in Action

4th Time - Suspend Account for 3 weeks MAX OR activate based on official request from Manager, impact PMP refer to Rating in Action

5th Time - Suspend Account, refer to Corporate Security for Investigation, Impact PMP refer to Rating in Action

Third-party Employee:



Corrective Actions :

2nd Time – Suspend Account for 1 week MAX OR activate based on official request from Manager

3rd Time - Suspend Account for 2 weeks MAX OR activate based on official request from Manager, Notification letter to Contractor Representative

4th Time - Suspend Account for 3 weeks MAX OR activate based on official request from Manager, Notification letter to Contractor Representative

5th Time - Suspend Account, refer to Corporate Security for Investigation, Notification letter to Contractor Representative

8. SUPPLEMENT II

Rating-in-Action Employees:

For All Employees	D	M	E	E+	S
Understands that the company technology assets, network and related information transmissions are the property of Saudi Aramco, and are monitored fully by the company and behaves accordingly	Regularly engages in technology use that violates the Information Security Acceptable Use Policy (GI 299.225) e.g. transmitting malicious software or material that violates Saudi laws or SA GIs; visiting inappropriate websites; posting indecent comments, or materials regarding the company	Periodically allows use of technology for personal use to interfere with business priorities and accomplishing work tasks	Never allows personal use of technology to interfere with business priorities and accomplishing work tasks	Never allows personal use of technology to interfere with business priorities and intervenes when others are misusing technology assets	Always acts in accordance with company expectations in terms of proper use of technology assets, intervenes when others are misusing technology assets and encourages others to behave similarly
Maintains a mindset of vigilance and spots potential fraudulent or phishing emails	Regularly fails phishing tests and shows no interest in improvement despite coaching from the supervisor (e.g. e-learning phishing modules)	Periodically fails phishing tests but is attentive to the need for improvement	Never fails phishing tests and needs no prompting to take cybersecurity seriously	Never fails phishing tests and regularly reports them as spam	Acts as a role model by never failing phishing tests, reporting them as spam, alerting, and educating others to spotting fraudulent or phishing emails
Seeks to keep abreast of cybersecurity and more general data security advancements and company policy	Shows no interest in the risks associated with cyber attacks and routinely fails to stay current in completing mandatory information security courses, and phishing assessments	Is generally aware of the risks associated with cyber attacks yet does not always stay current in completing mandatory information courses and phishing assessments	Is fully aware of the risks associated with cyber attacks and stays current in completing mandatory information courses and phishing assessments	Is fully aware of the risks associated with cyber attacks and encourages others to complete mandatory information courses and phishing assessments	Acts as a role model by sharing state-of-the art thinking and approaches relative to cybersecurity advancements
For Leaders Only	D	M	E	E+	S
Monitors cybersecurity metrics and processes of his/her group	Rarely monitors cybersecurity metrics and processes within his group	Sometimes monitors cybersecurity metrics and processes within his/her group	Monitors cybersecurity metrics and processes within his/her group most of the time	Consistently monitors cybersecurity metrics and processes and communicates them within his/her group	Champions cybersecurity metrics and processes within his/her group and identifies improvement areas