Saudi Arabian Mining Company (MAADEN)

Third-party and Supplier Cybersecurity Standard

Version 1

Effective date: 30 March 2025

Version Register

Version ID	Effective Date	Summary of Key Changes	Owner
001	10-03-2025	Initial version	Cybersecurity Department

Contents

1. Scope

Third-party and supplier cybersecurity standard provides the minimum cybersecurity requirements for Maaden third parties to protect Maaden from possible cyber threats and to strengthen third parties' cybersecurity posture.

2. Objectives

The controls in this document are applicable to third parties and suppliers engaged with Maaden or any of its business units, where the scope of engagement includes any of the following:

- Accessing, processing or storing Maaden non-public or personal data
- Providing or accessing a technology or communication asset
- Outsourcing of any material and business processes including cloud solutions or hosting services and websites

The controls in this document aim to effectively protect assets, critical facilities and data accessed, processed or managed by third parties through providing the required cybersecurity controls.

3. Third-party and Supplier Cybersecurity Controls

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

ID	Control Name
Cybersecurity Governance	
TP-1	The third-party must have a cybersecurity policy which is approved by the authorized officials and implemented.
TP-2	The cybersecurity policy must have an approved and implemented policy for Bring You Own Device (BYOD) with a minimum of the following: • Use of Mobile Device Management (MDM) solution • Restrict access to company resources • Secure wipe of company data when needed
TP-3	The third-party must perform annual assessments to ensure compliance with cybersecurity policies.
TP-4	Maaden reserves the right to undertake a cybersecurity audit on the third-party occasionally, or immediately in case of an actual or suspected security breach.
TP-5	The third-party must comply with applicable data protection and cybersecurity laws and standards, i.e., Saudi Personal Data Protection Law (PDPL), SADAIA National Data Management Office (NDMO), ISO27001, National Cybersecurity Authority (NCA) essential cybersecurity controls or any industry-specific standards applicable to the service(s) provided.
Risk Management	
TP-6	The third-party must conduct cybersecurity risk assessments in a regular basis to identify, analyze, remediate, and monitor risks. The scope of the assessments must include at least the following: • Technologies • Infrastructure

	• Change management • System integrations
Human Resources	
TP-7	The third-party must have a human resources policy covers cybersecurity requirements throughout the employment lifecycle, i.e., prior employment, on-boarding, during employment, and off-boarding. The requirements must include at least the following: • Screening/ vetting/ background checks • Non-Disclosure Agreements (NDA) • Cybersecurity responsibilities • Revoking of access permissions • Equipment and data return or secure destroy
Training and Awareness	
TP-8	The third-party must conduct cybersecurity training and awareness to employees and contractors in a regular basis. The third-party must maintain effectiveness of the conducted training and awareness.
TP-9	The cybersecurity training and awareness must include at least the following topics: • Email phishing • Acceptable use of technology assets and data • Secure web browsing • Social media security • Bring your own device (BYOD) security • Data privacy principles, data breach management, consent management and data subject rights • and the latest threat trends
Asset management	
TP-10	The third-party must maintain an up-to-date inventory of all hardware and software assets.

TP-11	The third-party must have an asset lifecycle management where cybersecurity requirements are defined and implemented.
TP-12	The third-party must have a process to monitor hardware and software assets against the following: • Unauthorized access to assets • Use of unlicensed assets • Use of end-of-support or end-of-life assets
Identity and Access Management	
TP-13	The third-party must have an identity and access management policy with at least the following: • Password length and complexity • Use of multi-factor authentication (MFA) • Access life-cycle management • Privilege access management • Access monitoring
TP-14	The third-party must have a formal process to detect and prevent unauthorized access to systems and data.
TP-15	The third-party must conduct periodic access reviews on accounts to ensure access remains in-line with the requirements.
TP-16	The third-party must ensure admin accounts are only used to perform administrative activities.
TP-17	The third-party must restrict remote access methods to prevent unauthorized connections to networks, systems, and applications.
Infrastructure Security	
TP-18	The third-party must have an endpoint security solution and ensure regular updates and scans are performed to detect and mitigate threats.
TP-19	The third-party must restrict connecting to untrusted networks, e.g., public Wi-Fi.

TP-20	The third-party must conduct secure configuration and hardening for systems. The scope of configuration and hardening must at least include the following: • Restriction of installing software except by administrative users • Restrict the use of removable media devices • Session management and lockout • Protection against malicious software and vulnerabilities • Deployment of latest security patches • Restrict connecting to untrusted networks • Disabling autorun/ autoplay and unnecessary services and features • Integrity monitoring • Countermeasures for end-of-life/ end-of-support systems.
TP-21	The third-party must conduct secure configuration of communication systems with at least the following: • Implementing SPF, DKIM, DMARK, and anti-spam for email servers • Restrict the use of public domains such as Gmail, Hotmail, etc.
TP-22	The third-party must monitor the capacity, availability and performance levels of infrastructure and network including DDoS, load-balancing, and capacity tests.
Network Security	
TP-23	The third-party must have an approved and implemented network security policy with at least the following: • Secure implementation of Domain Network Service (DNS) • Segregation of networks • Encryption of network traffic • DMZ and jump servers for remote access • Network monitoring
TP-24	The third-party must have physical or logical segregation and segmentation of networks to isolate critical systems, sensitive data, and corporate and guest networks.
TP-25	The third-party must have firewalls/ intrusion detection/ intrusion prevention systems to control ingress and egress network traffic.

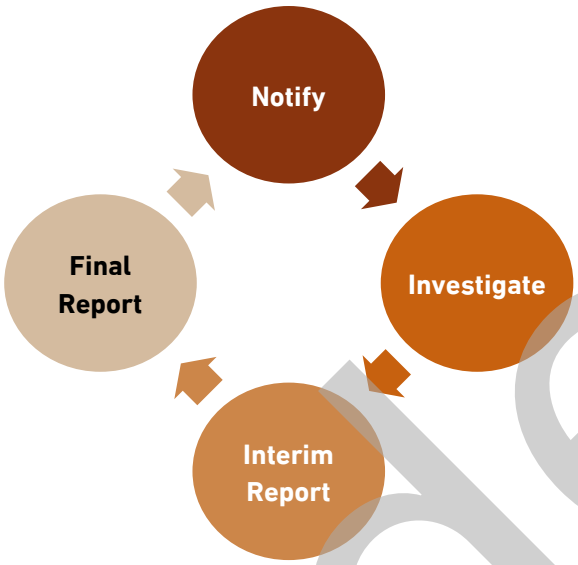
TP-26	The third-party must maintain a good security posture for external facing assets.
TP-27	The third-party must monitor and log networks and technology assets against unauthorized access or unauthorized activity. The logs must include the least of the following: • Logs are centralized and integrated with a SIEM solution • Logs are retained securely for at least twelve (12) months • Logs and events are reviewed and analyzed against compromise
Incident Management	
TP-28	The third-party must have an approved and implemented incident response and management policy with at least the following: • Roles, responsibilities, and escalation process are defined • Incidents are classified, tracked, and documented based on its criticality and risk level • Forensics are performed when applicable • Threat intelligent feeds for potential cyber threats
TP-29	The incident response capability must include preparation, detection and analysis, containment, eradication, recovery, documentation and preservation of evidence, communication protocols and lessons learned.
TP-30	The third-party must analyze threats against their cybersecurity posture and take corrective and preventative actions. Threats must include at least the following: • Assess threats against supply chain and remediation of risks • Share threat intelligence data with internal and external parties where required • Invoke incident/ crisis management when appropriated
TP-31	The third-party must notify Maaden within twenty-four (24) hours in case of discovering a cyber incident on the third-party or its supply-chain. Please refer to **Section 5** for the Cybersecurity Incident Notification.
Vulnerability and Patch Management	
TP-32	The third-party must conduct vulnerability scans and penetration tests in a regular basis covering at least the following: • Servers and databases

	• Networks • Internal/ external facing applications and systems
TP-33	The third-party must ensure that networks and key systems, applications, and servers undergo penetration testing by independent recognized external party at least annually.
TP-34	The third-party must ensure an up-to-date patching for technology assets and networks.
TP-35	The third-party must notify Maaden about known security vulnerabilities of supplied services. Accordingly, the third-party must support Maaden in the patching activities.
Data Protection	
TP-36	The third-party must have approved and implemented data protection policy which includes at least the following: • Data is classified based on its sensitivity • Data ownership • Data lifecycle management • Data access permissions • Data encryption at rest and during transfer • Data back-up and recovery • Data leakage prevention • Data retention and disposal • Segregation of data storage
TP-37	The third-party must perform a back-up on Maaden data where: • Back-up is encrypted through strong cryptographic algorithm • Back-up is segregated and protected in an offline environment • Back-up is tested frequently
TP-38	The third-party must store Maaden data in a segregated protected environment where access is restricted to specified and identified personnels.

TP-39	The third-party must securely return and delete or sanitize all Maaden data within 30 days of contract expiry or termination, unless a different retention period is specified in the contract. Confirmation of data destruction shall be provided upon request.
TP-40	The third-party must not store, process, or transfer confidential or personal data outside Saudi Arabia without written consent from Maaden.
Business Continuity	
TP-41	The third-party must have business continuity and disaster recovery plans that are approved, reviewed, and physically tested at least annually.
TP-42	The third-party must perform business impact assessments (BIA) on critical assets addressing the following: • Loss of critical or sensitive data • Operational disruption • Financial loss • Legal/ Regulatory compliance • Health and safety • Impact of a third-party disruption
Cloud Security	
TP-43	The third-party must have approved and implemented cloud security policy which covers at least the following: • Data protection measures • Security Monitoring • Data residency and cloud services • Shared responsibility model for third-party services • Data leakage prevention • Access control and management • Cryptography and key management • Vulnerability and patch management • DDoS prevention

TP-44	The third-party must ensure that all systems (i.e., servers, operating systems, applications, databases, networking, storage, virtualization, and security) related to Maaden are logically segregated from other client environments.
TP-45	The third-party must conduct scans against vulnerabilities, patches, configurations, unauthorized assets and unauthorized access in a regular basis.
Third-Party Security	
TP-46	The third-party must identify, assess, and manage cybersecurity risks associated with their supply-chain.
Physical Security	
TP-47	The third-party must restrict, monitor, and review the access to facilities for all staff including employees, contractors and visitors.

4. Cybersecurity Incident Notification



NOTIFY

The third-party must notify the Maaden Security Operations Center (SOC) within twenty-four (24) hours of any incident discovery. Notifications must be communicated through Maaden's cybersecurity SOC email (**CSIncidentAlerts@maaden.com.sa**). Please refer to **Appendix 5.2** for the incident notification template.

INVESTIGATE

This activity includes conducting a review of recent changes and modifications to Maaden systems and data with third-party access for any unauthorized modifications. Conduct a thorough review of the third-party's information for evidence of compromise.

INTERIM REPORT

The third-party is required to provide updates on the efforts to mitigate and resolve the incident every twenty-four (24) hours until the incident is resolved. The incident must be classified based on the Maaden incident classification outlined in **Appendix 5.1**. Please refer to **Appendix 5.3** for the interim report template.

FINAL REPORT

The third-party is required to provide Maaden cybersecurity team with two final reports for the incident as follows:

- Report intended for the Maaden Management with an executive summary of the incident, its cause, and the impact on Maaden. The report should be shared within three (3) business days of resolution or determining that the issue cannot be resolved within that time frame.
- The third-party is required to provide a detailed technical report of the incident including an executive summary of the incident. The report must contain a detailed compromise assessment and a corrective action plan. The report is to be shared with the Maaden cybersecurity team within ten (10) business days following resolution or determining that the issue cannot be resolved within that time frame. Please refer to **Appendix 5.4** for the report template.

5. Appendix: Incident Notification

5.1. Maaden Incident Classification

Classification	Description
Critical	Incidents causing serious damage directly affects the reputation and credibility of Maaden or affect many of Maaden's business units or business location significantly, requiring the activation of business continuity procedures.
High	Incidents causing a major interruption affects functional business units, key services or location.
Medium	Incidents with medium impact on the functioning of job units, sites or IT or OT assets, as well as a medium-to-high effect on non-critical business units in Maaden.
Low	Incidents with limited effect on a few resources. This includes cybersecurity incidents which can be tolerated for a certain period-of-time.

5.2. Incident Notification Form

Incident Notification Form			
Third-party name		**Focal point name**	
Incident date		**Focal point role:**	
Incident time		**Focal point email**	
Incident status		**Focal point phone number**	
Incident Overview			
How was the incident detected/ discovered?			
Incident category *(select one (1) option)*	○ Data Breach ○ Malware Infection ○ Unauthorized Access ○ Phishing Attack ○ Denial of Service ○ Insider Threat ○ Other. Please specify, (*write text here*)		

Incident description	

5.3. Incident Interim Report Template

Incident Interim Status Report		**Report No.: ###**	
Third-party name		**Focal point name**	
Incident date		**Focal point email**	
Incident time		**Focal point phone number**	
Incident Overview			
Incident current state	*(e.g., Ongoing, Resolved, Under Investigation, etc.)*		
Incident classification			
Incident type	*(e.g., Data Breach, Phishing, Malware, etc.)*		
Affected asset(s)			
Incident Description			
Known/ Suspected root cause			
Incident impact on Maaden	*(e.g., data leakage, service downtime, etc.)*		
Incident Response Action			
Action(s) taken			
Future action(s) to be taken			
Expected timeframe for full-service restoration			
Support Request			
Support needed from Maaden			

5.4. Incident Technical Report

Third parties must provide Maaden cybersecurity operations team with a technical report of any cybersecurity Incident within ten (10) business days of resolution or a determination that the problem cannot be resolved within this timeframe. Below is the template.

Incident Interim Status Report		**Report No.: ###**	
Third-party name		**Focal point name**	
Incident date		**Focal point email**	
Incident time		**Focal point phone number**	

Incident Overview	
Executive Summary	
Incident state	*(e.g., Ongoing, Resolved, Under Investigation, etc.)*
Incident classification	*Refer to Maaden Incident Classification*
Incident type	*(e.g., Data Breach, Phishing, Malware, etc.)*
Affected asset(s)	
Incident Description	
Root cause	
Incident impact on Maaden	*(e.g., data leakage, service downtime, etc.)*

Incident Details

The incident compromise assessment should include the minimum of the following:

- List of individuals and other Third Parties that were involved with any aspect of the incident handling
- When and how the incident was initially detected
- When and how the incident was initially reported to Maaden
- Description of impacted assets
- Description of incident impact on Maaden
- 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.)*
- Lessons learned
- Permanent corrective actions/ preventative measures *(What permanent corrective actions have been put in place as a result of this incident)*

6. Definitions

This section is a glossary that defines any uncommon terms used in this document. The table below shows the abbreviations used in this document with their corresponding definitions.

Term	Definition
Audit log	A chronological record of system activities. Includes records of system access and operations performed in a given period.
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.
Corporate Network	The Maaden computing resources and infrastructure.
Cybersecurity Assessment	Cybersecurity assessments include Risk Assessment, Compliance Assessment, Vulnerability Assessment and forensic analysis which ensure that the third-party is in compliance with cybersecurity controls in this standard and the contract.
Cybersecurity Incident	Unauthorized access, disclosure, modification or disruption of information, systems and services.
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.
Patch	A piece of software designed to fix operating system or software programming errors and Vulnerabilities.
Remote Access	Act of utilizing a remote access service, hardware or process to connect to a Maaden network or Maaden Systems.
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.
Third Party	Any external party: individual, business or organization that generates, acquires, compiles, transmits or stores data on behalf of Maaden.

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 surplused.
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 Maaden data.
Systems	A collection of communication and computing hardware, software, firmware, database and applications organized to accomplish a specific function or set of functions.
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 to apply a patch or fix to prevent a compromise and ensure adherence with the standard.
Assets	Anything that has value to Maaden 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.
Critical Facilities	A physical location housing information processing systems such as data centers, communications closets, or cabling (power, network etc.).
Critical Data	Maaden confidential data that if leaked or lost would result in high risk and adverse impact to Maaden including but not limited to brand reputational damage, financial loss, operational impact, loss of proprietary information, or loss of competitive advantage.
Cybersecurity	The mandatory minimum information security requirements to support the protection of confidentiality, integrity, and availability of Assets.
Cybersecurity Risk Assessment	The overall process of calculating the potential impact of an event using metrics-based risk identification, analysis and evaluation.
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.

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 Maaden'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.
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 Service	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.
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.
Technology Assets	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.