CATRION External Party Cybersecurity Policy

Effective: 14.01.2025 Version. 04

1 INTRODUCTION

This policy aims to define Cybersecurity requirements to ensure the protection of information and technical assets of Catering Holding Company (CATRION) from Cybersecurity risks related to external parties, including support services for information technology and services managed in accordance with the company's policies and regulatory procedures.

This policy follows the national legislative and regulatory requirements and relevant international best practices of the Essential Cybersecurity Controls (ECC-2: 2024) and any other related controls issued by the National Cybersecurity Authority (NCA) that are applicable to CATRION, such as Cloud Cybersecurity Controls (CCC-2:2024). The Cybersecurity Policy identifies and highlights the areas of concern, which must be addressed by External Parties.

2 SCOPE:

This policy applies to all CATRION external parties including their personnel, outsources, and sub-contractors who provide good or services, or have access to CATRION data, systems, applications or network.

3 DEFINITIONS:

3.1 CATRION:

CATRION for Catering Holding Company

3.2 Cybersecurity:

The protection of networks, IT systems, operational technologies systems and their components of hardware and software, their services, and the data they contain, from any penetration, disruption, modification, access, use or unauthorized exploitation. The concept Cybersecurity also includes information security and digital security.

3.3 NCA:

The National Cybersecurity Authority in Saudi Arabia.

3.4 External Parties:

Any external or third-party entities that have a current contractual relationship with CATRION, or that is being considered for contractual relations.

3.5 Endpoint devices:

Endpoint devices are any devices that connect to a network and serve as points of entry or exit for CATRION data. This includes computers, servers, smartphones, tablets, printers, and any other devices that communicate with the network.
Endpoint devices may be supplied by CATRION or utilized by vendors and their subcontractors.

3.6 Critical Systems:

Any system is defined as critical by CATRION.

The term "Confidential Information" as used in this policy includes, but is not limited to:

- trade secrets.
- technical materials, data, and information.
- product information and roadmaps.
- bid data and transaction information.
- CATRION staff personal information and details.

- customer lists.
- compilations of information, financial information, or specifications that are used in the operation of CATRION's business or that may eventually be used in the operation of CATRION's business; and
- other information relating to the CATRION's business that is not public knowledge.

4 POLICIES TO BE APPLIED BY EXTERNAL PARTIES:

All external parties, and their subcontractors shall ensure applying below Cybersecurity requirements where applicable based on the nature of the external party scope of work.

4.1 General Requirements:

4.1.1 Comply with all regulations and requirements of the National Cybersecurity Authority (NCA), as the legitimate authority in Saudi Arabia.

4.1.2 Comply with the related laws, regulations, and organizational policies and procedures of CATRION.

4.1.3 NDA to be signed if any confidential information to be shared before the agreement.

4.1.4 Sign CATRION contract template, otherwise, provide CS GRC team a copy before signing the contract to check any missing CS requirements to be included.

4.1.5 Password protection measures must be enforced within the external parties' environment. including, but not limited to, minimum password length, complexity, and periodic password updates.

4.1.6 Any critical and/or confidential information must be protected and shouldn't be disclosed unless there is an absolute necessity to protect CATRION from a catastrophic loss.

4.1.7 Multi-Factor Authentication (MFA) must be enforced on all remote access and all cloud services access.

4.1.8 Immediate notification to CATRION is required when employees using CATRION user credentials undergo transfers, re-assignments, or terminate their employment.

4.1.9 External parties must foster a Cybersecurity-centric culture by implementing regular awareness and training programs to ensures comprehensive understanding and adherence to Cybersecurity protocols among their personnel, enhancing overall resilience against potential threats.

4.1.10 External parties' personnel who require access to CATRION systems or networks must complete Cybersecurity awareness provided by CATRION before being granted the required access.

4.1.11 External parties' personnel must use the email in a responsible, effective, lawful, and secure manner.

4.1.12 The external parties' personnel must not use personal emails for any work related to CATRION.

4.1.13 Save Cookies and Credential feature must not be used or allowed in web browsers.

4.1.14 External parties must use the latest operating systems and ensure that patch management is up to date. Software and antivirus updates should be applied where and when possible. Daily updates and weekly updates should be performed consistently.

4.1.15 Anti-spam protection, along with the Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting & Conformance (DMARC), must be implemented on email domains within the DNS server.

4.1.16 External parties shall securely return all forms of CATRION data including backups unless CATRION formally requested that such data be destroyed. Such return or destruction shall be within a maximum of fourteen (14) days after the conclusion of the agreement. Within this fourteen (14) day period, the external party shall certify in writing to CATRION that such return or destruction has been completed. The sanitization must be conducted in alignment with industry best practices.

4.1.17 External parties and cloud service providers must ensure the return of data in a usable format, and it is irreversible removal upon termination or expiry of the service using the latest industry specialized software available. This includes a guarantee of data retrieval and deletion in a manner that it is non-recoverable, ensuring the complete and secure cessation of access to the data by any party.

4.1.18 All endpoint devices must have firewalls and be configured and enabled.

4.1.19 External parties must manage their cybersecurity risks.

4.1.20 CATRION has the right to conduct risk assessment on the external party's environment and the provided services or products.

4.1.21 The external party must cooperate and implement the risk mitigation plans to mitigate the identified risks based on the CATRION risk assessment result.

4.1.22 Generic accounts must not be allowed, and unique passwords and credentials should be issued to the employees, especially ones who are dealing with CATRION.

4.1.23 External parties should limit and review privileged accounts on a regular basis.

4.1.24 Remote access to the hosting infrastructure must be controlled.:

4.1.24.1 Remote administrative access to CATRION services or data must not be allowed. Any exceptions require an approved waiver.

4.1.24.2 Remote access, whether administrative or regular access, by a third-party personnel to CATRION on-prem resources must be through site-to-site, or client-to-site VPN.

4.1.24.3 Remote access, whether for administrative or standard use, by third-party personnel to CATIRON's cloud-based resources is only permitted after the third party's IP address has been whitelisted.

4.1.24.4 All remote access sessions by external party's personnel to CATRION information systems and networks are subject to monitoring. At minimum, for each login the date, time, and username will be recorded. System records will also show the last time someone logged in and whether there were any access failures.

4.1.25 External parties must ensure that all communications between their servers and the CATRION's servers are secured with HTTPS to protect data in transit.

4.1.26 CATRION data should only be shared with authorized individuals who are part of the work scope given.

4.1.27 CATRION data and confidential information must be kept in a secure place with limited access to only authorized employees.

4.1.28 Plain-text passwords should not be used in any CATRION applications.

4.1.29 External parties should have disaster recovery plan in place and be ready in case of disaster occurs and must inform CATRION immediately in case any of CATRION data compromised.

4.1.30 CATRION data and confidential information in critical systems - which are handled by external parties - should not be transferred outside the production environment.

4.1.31 CATRION's information and personal data residing in critical systems must not be processed, stored, or used in the testing environment unless restrict controls are applied to protect such data, such as data masking, data scrambling, or data anonymization, regardless of consent.

4.1.32 An appropriate business continuity plan within the external party environment should be developed and communicated to CATRION to avoid the lack of services provided to CATRION.

4.1.33 Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) must be implemented at the external party network level.

4.1.34 In case of hosting an application or a website for CATRION, Web Application Firewall (WAF) must be implemented to check incoming traffic for possible threats and malicious activity.

4.1.35 In case of hosting an application or a website for CATRION, a Distributed Denial-of-Service (DDoS)/DOS protection solution must be implemented on the outer edge (network perimeter) to safeguard against potential attacks, ensuring the availability and reliability of the services

4.1.36 External parties must develop approved procedures to grant and revoke access to all information and technology systems that process, transmit, or store CATRION's information, in line with CATRION's cybersecurity requirements and the objectives the cybersecurity controls.

4.1.37 External parties must review access rights regularly.

4.1.38 Audit records must be securely stored, maintained, and made available at CATRION's request and as per the relevant legal and regulatory requirements.

4.1.39 External parties must follow the formal and appropriate change management process.

4.1.40 The concerned parties in CATRION must be informed of any significant changes that are planned in relation to the storage or transmission of CATRION data.

4.1.41 In case the sharing of confidential data and information is required between the two parties before signing the contract, external parties must sign a Non-Disclosure Agreement.

4.1.42 During the bidding process, external parties must register into CATRION E-Bidding System to review and sign the required documents such as Cybersecurity Declaration and Authorized Signatories.

4.1.43 During and after the engagement, both personnel of CATRION and external parties must not divulge or share any confidential information or data outside the scope of the engagement to non-authorized people.

4.1.44 External parties to have policies to limit session durations to avoid prolonged inactive sessions on the website, system, and application.

4.1.45 Enabling automatic logout after a period of inactivity ensures the security of the system, website, application, and workstations, including PCs and servers...etc., during use.

4.1.46 External service providers must have a documented service level agreement (SLA) that is shared and reviewed by the Cybersecurity department at CATRION.

4.1.47 Incident and response SLA should be providing contact information for any incident owner

4.1.48 External parties should backup CATRION data and information and must ensure that backups of systems are performed and tested to ensure recoverability of data.

4.1.49 SLA between CATRION and external party must specify a return time for data in case of complete disaster based on data classification.

4.1.50 External parties must grant CATRION the necessary permissions to conduct tests to verify the external parties' compliance with CATRION 's cybersecurity requirements and provide the required reports when needed.

4.1.51 Encryption of CATRION sensitive information in backups.

4.1.52 External party must not utilize tools to bypass CATRION security systems.

4.1.53 External party must conduct periodic penetration testing to test all internet facing web applications and their components in the hosting infrastructure

4.1.54 If any external party is hosting CATRION services or data, the identified findings must be addressed and resolved.

4.2 General Requirements of Cloud Service:

4.2.1 Comply with NCA Cloud Cybersecurity Controls (CCC).

4.2.2 Agreement between the cloud service provider and CATRION on the cloud computing roles and RACI assignments.

4.2.3 Before hosting or storing data on cloud computing or hosting services, external parties must provide support and cooperation with CATRION to classify the data appropriately. This classification ensures adherence to prescribed data handling practices, facilitating the secure storage and management of information based on its sensitivity and regulatory requirements.

4.2.4 Use of Cloud Computing services shall comply with all Regulatory privacy laws and regulations, and appropriate language be included in the contracts defining the Cloud Computing source responsibilities for maintaining privacy requirements.

4.2.5 Independent reviews and assessments shall be performed on the cloud hosting service.

4.2.6 Cloud service providers must ensure that all hardware and software components in their environment have up-to-date vulnerability and Patch management process that in line with NCA regulations and best practices.

4.2.7 Cloud service provider shall have Antivirus software with a defined update mechanism.

4.2.8 Cloud service provider shall have an up-to-date Access management process that in line with NCA regulation and best practices.

4.2.9 Mandatory for admin user access.

4.2.10 Cloud service provider shall have hardening for Operating Systems and database before deployment.

4.2.11 Cloud service provider shall have Background check for users with high privilege and administrative rights.

4.2.12 Cloud service provider shall have Physical security and access controls to prevent unauthorized access.

4.2.13 Cloud service provider shall have USB ports being physically secured or disabled on the hosting servers.

4.2.14 CATRION's environment within cloud computing services must be logically or physically separated from other entities' environments. This segregation ensures distinct boundaries, preventing unauthorized access or interference between different entities' data and systems within the cloud environment, thereby upholding data integrity and security.

4.2.15 Cloud service provider shall not access and/or use CATRION’s data for any secondary purposes.

4.2.16 Data Center of Cloud Service Provider should be certified by an internationally/national recognized entity.

4.2.17 Implement a disaster recovery and business continuity procedures related to cloud computing with the cooperation of CATRION IT department and Cybersecurity department.

4.2.18 Data transmitted to, stored in, or transmitted from cloud services must be encrypted. This encryption aligns with pertinent laws, ensuring the secure handling of data throughout its lifecycle within cloud environments, safeguarding it against unauthorized access or breach

4.2.19 Logging and Monitoring must be implemented for all Infrastructure components such as firewalls, routers, servers, applications, etc.

4.2.20 Monitoring of the infrastructure components and applications for any adverse activity or attacks.

4.2.21 Alerting and incident response mechanisms to ensure remedial action can be taken promptly and shall notify CATRION if there is any incident that may affect the CATRION’s applications and assets.

4.2.22 The cloud service provider must ensure a detailed exit strategy is defined and agreed upon with CATRION

4.2.23 All system updates or changes must be tested in a testing environment before they are deployed to the live production systems.

5 <u>Data Security:</u>

5.1.1 Comply with all regulations and requirements of the Saudi Data & AI Authority (SDAIA) Personal Data Protection Law (PDPL), as the legitimate authority in Saudi Arabia.

5.1.2 External parties must maintain high standards of data security and ensure the protection of CATRION’s sensitive data from unauthorized access or disclosure.

5.1.3 The implementor cannot use production and real data in testing environment specially those related to our customers. Dummy data to be used prior migrating real ones.

5.1.4 External parties associated with services require processing of Personal Data for CATRION must assign a Personal Data Protection Officer whom responsible to provide the assurance of protecting personal data.

5.1.5 Data generated from engagements with CATRION and not publicly available must not be used by external parties to develop new services or for benchmarking without CATRION's approval.

5.1.6 Where AI or Machine Learning services are used, cloud service provider shall ensure that models and algorithms comply with ethical standards and regulatory requirements, including transparency and bias mitigation.

5.1.7 Encryption of data at rest, and Secure Key Management process to manage private keys.

5.1.8 Ensure access control process in place to prevent administrative users e.g. operating system, database and application administrators from accessing company`s data.

5.1.9 A defined data handling process to prevent company`s data from being transferred outside the approved cloud instance.

5.1.10 Strong database encryption for databases containing sensitive information, using the following as Minimum length requirements for the encryption keys:
•Triple-DES – 128 bits.
•AES – 256 bits.
•RSA – 1024 bits.

5.1.11 All CATRION's data must be hosted and stored in countries with established regulations for privacy, data security, and cybersecurity.

5.1.12 All CATRION's data must be documented/logged prior hosting or transfer.

5.1.13 Prior going live, external parties must provide notification to any changes being made to the product or service (Patch Updates, changes in infrastructure, relocation to a different region, use of subcontractor)

5.1.14 External parties must notify and obtain approval from CATRION prior sharing any CATRION data to a subcontractor.

5.1.15 External party must be responsible for managing and mitigating all risks associated with any subcontractors they are engaging with. Ensuring that subcontractors comply with all relevant contractual obligations, policies, and standards applicable to this agreement.

5.1.16 External parties providing software development for CATRION must establish an escrow facility using a trusted provider.

5.1.17 External party must support CATRION in the event of legal action that involves CATRION information handled by the external party.

5.1.18 External party must encrypt CATRION data while in transit, and during in sit.

5.1.19 External party must implement data validation on all input fields to only accept input with valid data type, syntax, and length

5.1.20 External party must have a procedure for off-boarding, in-boarding their personnel which includes granting and removing access to assets.

5.1.21 Non authorized devices must not be used to store, process, or access CATRION assets.

6 INCIDENT REPORTING:

6.1 External Parties must report immediately any Cybersecurity incidents or data breach that may affect CATRION data or effect the service provided by the external party to CATRION Cybersecurity Team Email: Cybersecurity@catrion.com and include the following information:

6.1.1 Date of incident:

6.1.2 Type of incident:

6.1.3 Classification of incident:

6.1.4 Was CATRION data compromised?

6.2 External party may escalate the matter to Cybersecurity Head within CATRION if required.

6.3 External parties must provide a written report on any Cybersecurity incident within 72 hrs. from detecting the incident to CATRION.

6.4 In the event of an incident, CATRION's Cybersecurity Team will promptly inform the external party, expecting their cooperation and necessary support and provide required event logs. This collaborative approach ensures swift resolution and mitigation of the incident, with the external party providing essential assistance as required to address the situation effectively.

7 DEVIATIONS:

7.1 In case the compliance with this policy is not technically feasible, a waiver must be requested.

8 REVISION:

8.1 This policy will be reviewed, and updated annually or as required, by CATRION Cybersecurity Department, to ensure that it continues to meet the business and regulatory requirements. Updates to this policy will be communicated to the external party where a significant requirement is implanted