Security Standards for MetricStream Cloud

Information Security

Author: Madhu Shankarpani

Doc Version: Ver 1.3

Effective Date: 20-Jan-2026

Last Revised Date: 09-Jan-2026

Document Control

Change Record

Date	Author	Ver	Comments (if any)
01-Apr-22	Madhu Shankarpani	1.0	First issue
05-Sep-22	Lovey Lukose	1.1	Modified
15-Nov-23	Lovey Lukose	1.2	Modified
09-Jan-26	Lovey Lukose	1.3	Modified

Reviews

Date	Reviewer	Ver	Comments (if any)
01-Apr-22	Thien Dinh	1.0	-Reviewed-
14-Nov-22	Thien Dinh	1.1	-Reviewed-
08-Jan-24	Thien Dinh	1.2	-Reviewed-
13-Jan-26	Thien Dinh	1.3	-Reviewed-

Approvals

Date	Approver	Ver	Comments (if any)
01-May-22	Larry Bump	1.0	-Approved-
14-Nov-22	VN	1.1	-Approved-
11-Jan-24	VN	1.2	-Approved-
20-Jan-26	VN	1.3	-Approved-

Contents

MetricStream Cloud Security Standards

1 Introduction

Confidentiality, integrity, and availability forms the basic tenets of security of information management by protecting information systems from unauthorized access, unauthorized alterations, or deletions, and providing uninterrupted service to customers. MetricStream strives for the highest level of security with its multilayered approach. MetricStream has implemented security tools and policies and employs best practices to keep its cloud environment secure and protect the data of its customers. With ISO 27001 certification, SOC 2 Type II and HIPAA attestations, MetricStream's information security posture meets industry standards such as OWASP, CIS, NIST, DORA and its customer instances are protected.

This document sets forth the minimum-security standards for the MetricStream Cloud/SaaS platform, that is provided under Customer's SaaS agreement with MetricStream ("Agreement"). This document describes the security, data protection, and business continuity standards for MetricStream.

As part of its Privacy and data protection commitments, MetricStream can execute Data Processing Agreement (DPA) and EU Standard Contractual Clauses (SCCs) for international data transfers, that is inline with GDPR and other international regulations.

MetricStream's Privacy Statement: `https://www.metricstream.com/about-us/privacy-policy.htm`

Unless otherwise defined herein, all capitalized terms used in this document shall have the same meaning outlined in the Agreement (or its other appendices) or to which this document is appended to.

2 General Requirements

(2.0.1) MetricStream shall fulfill and comply with all information security, data protection and business continuity requirements, relevant standards, applicable legal and regulatory operational resilience requirements set forth in this document. MetricStream is responsible for creating and maintaining documentation that describes in detail the controls implemented by MetricStream to meet the above requirements.

(2.0.2) MetricStream shall track changes to relevant laws, regulations and standards and update its own processes to comply with them.

(2.0.3) MetricStream shall safeguard Customer's information located in and related to the Services delivered by MetricStream, including MetricStream's GRC SaaS applications and platform, as well as

any information otherwise used or transferred to MetricStream or third parties acting on its behalf. MetricStream shall not provide third parties to gain or access the information unless explicitly authorized by Customer, in advance, in writing.

2.1 Security and Risk Management

(2.1.1) MetricStream shall establish and maintain an Information Security Management System ("ISMS") that is approved by MetricStream's executive management. The ISMS will be reviewed and updated annually.

(2.1.2) MetricStream shall have documented standards and procedures for managing ICT risks identified, assessed, and monitored with specific consideration of operational disruption, concentration risk, and systemic impact, that will apply across the organization.

(2.1.3) MetricStream shall name the person(s) responsible for reporting all security related matters related to procured service that affects the Customer. Upon request, once annually and upon 60 days prior written notice or email, MetricStream will provide a Security report to Customer, at Customer's cost or as agreed upon in the Agreement.

2.2 Personnel Security and Training

(2.2.1) MetricStream shall have an established Human Resources process, that includes hiring and screening, transfer, and contract termination processes to prevent unqualified or unauthorized personnel to participate in the provision of the services provided by MetricStream ("Services").

(2.2.2) Each of MetricStream's employees (including consultants, temporary agency workers, partners, and other external resources) shall sign a non-disclosure agreement ("NDA") with MetricStream.

(2.2.3) Each employee shall be given adequate security and privacy awareness and trainings relevant to their duties, as part of their onboarding. Additionally, security and privacy training shall be given annually.

2.3 Information Classification and Handling

(2.3.1) MetricStream shall have an information classification scheme as per MetricStream's asset management procedure, that applies across the organization and covers information in all formats (physical, electronic, etc.).

(2.3.2) The information classification scheme shall specify the classification levels of confidentiality of information and provide description of each level of confidentiality.

(2.3.3) All Customer instances in production and data shall be classified as Confidential.

(2.3.4) MetricStream shall have a documented process for handling the information throughout its life cycle, storage, retrieval, modification, and destruction.

(2.3.5) Customer information in physical or electronic form, shall be destroyed using secure means of disposal methods, upon Customer's request during contract termination or when no longer required.

2.4 Data Management

(2.4.1) The GRC applications, functionalities or processes related to the Services, shall incorporate security controls that protect the confidentiality, integrity, and availability of Customer's data.

(2.4.2) There is NO co-mingling of data across customers since each customer is deployed as single-tenant model.

(2.4.3) MetricStream shall encrypt all sensitive data in transit (AES-256) and at rest (TLS 1.2 or above). Backups are also encrypted.

(2.4.4) Encryption keys shall be stored in a Key Management System ("KMS").

(2.4.5) Encryption keys are managed via key management service and automatic annual rotation. Customer-Managed Key (BYOK) options are available for customers upon request.

(2.4.6) Customer data is stored within the customer's selected data residency region, as agreed in the Master Services Agreement. The data does not leave the selected region without acustomer consent, except as required by applicable law.

2.5 Logical and Physical Access Controls

(2.5.1) MetricStream's access rights management procedures shall be defined, and access rights given based on roles and responsibilities, based on the principle of 'least privilege'. Access to MetricStream's Service delivery premises shall also be controlled.

(2.5.2) MetricStream's Service delivery premises shall be physically protected against unauthorized entry. This includes network devices, connections, and routing points. Premises shall have surveillance for detecting and recording such attempts.

(2.5.3) MetricStream shall monitor access to its secured premises using badge access reports.

(2.5.4) All assets included in the scope of the Services shall be recorded and such assets shall be properly protected (ownership of assets, acceptable use, classification, and handling), including the

information transmitted from the assets. Critical ICT assets and supporting cloud services are identified and mapped to business functions. Information that is transmitted by the Customer will be considered confidential by default, if no other classification has been assigned to the document or information.

(2.5.5) MetricStream shall require all users are assigned with a unique ID. This unique ID must allow tracking who is accessing which premises or any of the secured assets relating to the Services or the Agreement.

(2.5.6) Access Roles shall be separate for end user and privileged users so that access rights do not create such work combinations, that could present higher than normal risks of misconducts, abuse or heighten the risks arising from negligence or mistakes. Access rights are removed when the need for them no longer exists.

(2.5.7) Access rights related to Cloud Infrastructure shall be reviewed periodically and all unnecessary or dormant users, roles and rights shall be disabled or removed. For application access for MetricStream users, MetricStream shall request the customer's Application Administrator as per the process agreed with the Customer.

(2.5.8) MetricStream shall apply multi-factor authentication (MFA) to remotely access the services infrastructure and for all privileged access to production systems, cloud management consoles, and administrative application access.

(2.5.9) MetricStream implements Privileged Access Management (PAM) controls including just-in-time (JIT) access provisioning, session recording for all administrative access to production environments, and quarterly privileged access reviews.

2.6 Security of Operations

(2.6.1) MetricStream shall have procedures in place for the removal, disposal or reuse of equipment/media and the protection of equipment/media off premises.

(2.6.2) MetricStream shall have operating procedures applicable to the Services and the Services environment that are formally documented, including all changes made throughout the course of operations.

(2.6.3) MetricStream shall have proper segregation of duties to mitigate the risk of fraud and other misconducts or abuse. MetricStream shall regularly review (e.g., at least once per year) the application of the segregation of duty controls.

(2.6.4) MetricStream shall have its development, test and production environments separated and those environments that host customer data are properly isolated from other environments used by other customers of MetricStream.

(2.6.5) “Segregation of duties” principle shall be followed in application development, application Support, infrastructure operations management life cycles so that the roles and job responsibilities are clearly separated.

(2.6.6) MetricStream shall not use production or Customer data in the development process unless written approval is obtained from Customer.

(2.6.7) MetricStream shall restrict and limit access to the Customer’s information assets as per the Information Security policy.

(2.6.8) MetricStream shall remove or change all default system level administrator user IDs and passwords and remove unnecessary services from hardware and software components which have been installed. All hardware and software components shall be free of malware and protect them with maintained malware protection. MetricStream shall have secure configuration baselines for all components such as operating systems, databases, routers, or switches.

(2.6.9) MetricStream shall configure all systems to synchronize with NTP servers.

(2.6.10) For any changes required in the Services provided, a formal change management process (in accordance with ITIL requirements) is applied, including a formal system acceptance process. Customer shall be informed of significant changes without undue delay.

(2.6.11) MetricStream's infrastructure is protected against distributed denial-of-service (DDoS) attacks using DDoS protection services, DNS security controls, and ingress/egress filtering. Traffic anomaly detection triggers automated mitigation.

(2.6.12) MetricStream has Network and Security Operations centers in place to monitor the availability, performance and security of the GRC SaaS services.

2.7 Suppliers

(2.7.1) MetricStream shall notify Customer of Suppliers used by MetricStream to provide the Services for Customer or suppliers that have access to Customer’s data, premises, or information. The information shall include what data MetricStream processes and in which role. MetricStream shall have suppliers follow the requirements set forth in this document.

(2.7.2) The Suppliers are risk assessed prior to onboarding and monitored continuously based on criticality.

(2.7.3) Contracts with Suppliers would include, as applicable, audit rights, incident notification obligations, data location transparency, and subcontractor disclosure requirements.

2.8 Artificial Intelligence & Machine Learning models

(2.8.1) MetricStream's AI and ML models are Opt-In for customers (Customers must explicitly sign up to enable the AI features in the Product)

(2.8.2) AI workloads shall be deployed within approved cloud subscriptions/accounts under centralized governance.

(2.8.3) Public network access to AI model endpoints shall be restricted unless explicitly approved.

(2.8.4) AI systems shall operate within documented and approved use cases.

(2.8.5) The models are built on industry grade AI services on the Cloud hyperscalars. These AI services provides only the infrastructure to train/ host models and does not automatically scrape or collect customer data.

The models are trained on specific customer data and deployed individually for the respective customer. AI training and inference workloads shall be deployed only in approved cloud regions.

(2.8.6) Data used for AI model training or inference shall be classified and handled according to data protection policies. Data minimization principles shall be applied to AI training datasets.

(2.8.7) There is NO co-mingling of data across customers since each customer is deployed as single-tenant. The data is encrypted, and any third party would not be able to access the data.

3 Secure Development and Maintenance Standards

Activities listed in this document are applicable for MetricStream owned/managed systems where Customer's information is processed. This applies to MetricStream's out-of-the-box solution. By the very nature of the application's configurations, extensions, and customizations, responsibility for MetricStream's Web Application security is shared between Customer and MetricStream. The

MetricStream Web Applications are designed with Secure SDLC principles and validated via SAST, DAST, SCA, and application penetration testing for major releases.

Customer Responsibilities: Customers are responsible for application configuration, user access administration, API key management, integration security, and browser and endpoint security.

For more information, visit https://www.metricstream.com/shared-responsibility-and-cloud-security

3.1 General Requirements

(3.1.1) MetricStream will oversee setting up and maintaining all required security test environments as well as data required for conducting the security testing.

(3.1.2) MetricStream shall use industry standard tools and methods to both manage (e.g., tracking and tracing of security requirements) and test security (e.g., code vulnerability test).

(3.1.3) "Segregation of duties" principle shall be followed during the application development and/or maintenance life cycle so that e.g., various environments (development, test, and production) are separated and that developers do not have direct access to code or data in production. In case MetricStream is using a model for development where the segregation of duties principle cannot be followed, MetricStream shall present its risk assessment and controls that support the agile way of working. These controls shall be accepted by the Customer so that no individual is able to deploy changes in the production singlehandedly. The implemented controls shall rely heavily on automation as applicable.

(3.1.4) Security and data protection are built-in to the application development and maintenance processes.

(3.1.5) MetricStream shall document and maintain its Secure Development Life Cycle ("SDLC") and server hardening instructions. MetricStream shall conduct regular information risk assessments for target environments (e.g., critical business environments, processes, and applications) at least annually, as well as independent and regular audits. The results of audits and/or certification will be presented to the customer upon written request, once annually.

(3.1.6) MetricStream is responsible for the security of the developed applications and/or functionalities throughout its lifecycle (from its development to operation to its decommissioning or shutdown) as well as for the security of its maintenance activities and the results of such maintenance activities.

3.2 Vulnerability Management

(3.2.1) MetricStream is expected to track and stay informed on vulnerabilities related to the provided Services as well as to monitor the security and lifecycle management of the Services. MetricStream's personnel shall stay up to date with security vulnerabilities, tracking new attacks, threats, and risks, and following security trends.

(3.2.2) MetricStream shall communicate all critical and high vulnerabilities exceeding specified remediation timelines, related to the Services to the Customer.

3.3 Vulnerability Scanning

(3.3.1) Information systems will be regularly checked for compliance with security implementation standards. Monthly vulnerability assessments are carried out. Identified vulnerabilities during a scan will be closed as given as follows:

- Critical vulnerabilities will be closed as soon possible without any undue delay and undergo another vulnerability assessment to verify the closure.
- High severity vulnerabilities will be closed within 30 days and must undergo another vulnerability assessment to verify the closure.
- Medium and low severity vulnerabilities will be closed based on impact to the Customer's service.

3.4 Log Management

(3.4.1) Systems used by MetricStream to process Customer's data shall produce sufficient and accurate audit logs that can address the following:

- A request must be recorded independently of processing it.
- Time of the server where logging takes place must be synchronized with centralized time server (NTP).
- MetricStream shall present the redacted log files regarding the handling of the Customer's data if requested to support the Customer in security incident resolution.

3.5 Log Retention Period

(3.5.1) Application and security logs are retained for a minimum of 12 months online and 24 months in archive storage, which is consistent applicable regulatory requirements. Extended retention is available based on customer requirements by agreement and at a cost.

(3.5.2) Log data is stored securely with access controls and integrity protection.

3.6 Risk Assessment

(3.6.1) MetricStream shall perform a risk assessment for all new applications and/or functionalities or critical application changes used to process Customer's data.

(3.6.2) Depending on the type of the application and/or the new functionality to be implemented, MetricStream shall evaluate potential threats and risk of misuse of the application and/or new functionality.

3.7 Control Requirements and Control Design

(3.7.1) Based on the results of the risk assessment referred to in Clause 3.6 above and the sensitivity of information processed in the application, MetricStream shall design and implement the required security controls.

3.8 Security Testing

(3.8.1) MetricStream is responsible for conducting security testing and fixing security defects impacting Customers' security posture in the Services and/or in any applications, functionalities or processes relating thereto per the shared responsibility model.

(3.8.2) MetricStream shall conduct both manual testing and automated testing to validate the code relating to any software that is, or is intended to, process Customer's data in connection with the Services.

3.9 Security Auditing

(3.9.1) Before delivering any new or upgraded Customer systems (e.g., applications, servers, database, etc.) and/or functionality release to production, MetricStream shall perform a security review/ assessment of the instance. The requirement is applicable also for any major change that impact in degrading the security measures in the developed cloud systems (e.g., applications, servers, database, etc.) or the Services provided. MetricStream is required to fix deficiencies identified within reasonable time from the review/ assessment.

Once annually, MetricStream will request a third party to conduct an independent security review of the major release of the Application as well as MetricStream's cloud environment that are in line with standards such as CREST, PTES, OWASP WSTG.

4 Business Continuity and Disaster Recovery

4.1 Backups

(4.1.1) MetricStream shall establish backup and recovery procedures that cover both application and software backups as well as backups of all data processed relating to the Services or the Agreement.

(4.1.2) For application and/or software backups, MetricStream shall have an inventory of the necessary software required for mission critical functions and have backup copies with a offsite service. Software backups shall cover all components required to provide the Services in the event of a disaster or major incident

(4.1.3) Required documentation for operating and running each application shall be properly backed up and secured. Documentation shall include all activities required to operate the applications.

(4.1.4) Backup and recovery procedures shall be reviewed and tested at least once annually.

4.2 Business Continuity and Disaster Recovery

(4.2.1) MetricStream shall prepare for and mitigate risks that may cause long interruptions of the Services or seriously impact the Service infrastructure.

(4.2.2) MetricStream shall prepare business continuity and disaster recovery plans for the Services. MetricStream shall maintain readiness to act according to these business continuity and disaster recovery plans for the Services.

(4.2.3) Business continuity and disaster recovery plans shall be reviewed and annual resilience testing of critical ICT systems shall be executed for disruption scenarios to validate operational continuity that are in line with regulations such as DORA.

(4.2.4) In case a disaster or major Incident is declared, MetricStream shall activate its business continuity processes, inform the Customer thereof, and provide a single point-of-contact to coordinate with the Customer or their designee and all appropriate third parties.

(4.2.5) After the disaster or major Incident has ended, MetricStream shall provide a post declaration report (as needed) outlining what was done, what was the root cause of the incident and what lessons were learnt.

(4.2.4) MetricStream's GRC SaaS platform targets a Recovery Time Objective (RTO) of 24 hours and a Recovery Point Objective (RPO) of 6 hours for production environments. Actual targets may vary by service tier and are specified in the applicable Order Form or SLA Schedule.

5 Security Incident Response

5.1 Incident monitoring and reporting

(5.1.1) MetricStream shall monitor the Service infrastructure for security incidents affecting the maintenance and operations of systems and Services related to the Agreement ("Incidents"). Such Incidents are singular events or a series of linked events which have or may have a material adverse impact on the confidentiality, integrity, and availability of systems and services in scope.

(5.1.2) MetricStream shall report data breaches. Security incidents are classified according to defined severity thresholds, and ones associated with a data breach shall be treated with the highest priority and criticality.

5.2 Incident Notification

(5.2.1) MetricStream shall, in accordance with the process specified below, collect all relevant information, produce an incident report concerning Incidents and/or personal data breaches and submit it to the Customer.

(5.2.2) MetricStream shall contact Customer's Service Delivery manager or Customer's information security team when an Incident and/or personal data breach is confirmed within 24 hours. as soon as reasonably practical or as per supervisory authority notifications. However, if an Incident or a personal data breach requires the Customer's immediate attention or response, MetricStream shall contact the Customer without undue delay.

(5.2.3) MetricStream shall provide an initial report which shall contain headline-level information of the Incident and/or personal data breach and its foreseeable consequences based on the information available at that moment. Additionally, the initial report concerning personal data breaches shall consist of:

- the nature of the personal data breach.
- where possible, the categories and approximate number of data subjects concerned.
- and the categories and approximate number of personal data records concerned.

(5.2.4) MetricStream shall submit intermediate reports periodically as agreed with Customer's contact or MetricStream considers there is a relevant status update. MetricStream acknowledges that, in case of personal data breaches, submitting timely reports is especially crucial to enable Customer to fully fulfil its own notification obligations under applicable data protection legislation.

(5.2.5) MetricStream shall submit a final report of the Incident and/or personal data breach, including the root cause for supervisory review, within 2 weeks after submitting the initial report or as soon as the root cause has been determined.

(5.2.6) MetricStream shall assist Customer's authorized contacts with resolving the Incident and/or personal data breach as requested by Customer.

(5.2.7) MetricStream shall notify competent authorities within regulatory timelines for major ICT incidents

5.3 Contact Information

(5.3.1) Principal Contact from MetricStream in all cases is the Customer Success or Service Delivery Executive assigned to the service. In case of security incident affecting the Customer, MetricStream shall contact the Customer provided contact, Customer's representative specified in the Agreement or Customer's information security team (as applicable).

6 Compliance and Audits

(6.0.1) Once annually, Customer shall have the right to audit MetricStream's operations, premises, and processes to the extent they apply to the obligations under the Agreement, without affecting MetricStream's normal operations or business. Subject to at least forty-five (45) days prior written notice, Customer shall have the right to engage third parties in performing the audit (at Customer's cost), while excluding any MetricStream's direct competitors.

(6.0.3) Once annually, MetricStream shall provide Customer with SOC2 Type II report, ISO 27001 certificate or the executive summary of any Security review performed by an independent 3rd party, upon written request with 30 days' notice.

7 Disposition, Deletion, and Destruction of Customer Data

(7.0.1) On contract termination, MetricStream shall deliver to Customer all Customer's data, and other applicable service documentation or instructions according to the Agreement in an industry accepted machine-readable format.

(7.0.2) After delivering to Customer all data described in Agreement, MetricStream shall delete or destroy all Customer's data within 30 days except those required by applicable law or regulation. All equipment that contains or contained Customer's data shall be sanitized with data overwritten or securely destroyed according to industry standards.

(7.0.3) MetricStream shall deliver a report of the destruction of Customer information. If a system generated report is not available, a Letter of Destruction shall be provided and signed by a person with Management Authority.

(7.0.4) MetricStream shall inform Customer, if MetricStream has a legal responsibility to store certain Customer's information.