SECURITY AT XMATTERS

xMatters is an emergency communications provider and as such receives, stores and processes Personally Identifiable Information (PII) and other client data as part of its platform services. xMatters Software as a Service (SaaS) operates in a Java environment that resides in Google Cloud Platform (GCP). The following document describes the technical and security measures implemented by xMatters for secure handling of clients' data.

November 2020

Security Framework

The xMatters Information Assurance Team manages a robust Information Security Management System (ISMS), which is certified against the following industry standards:

ISO 27001:2013	Information technology – Security techniques – Information security management systems – Requirements
ISO 27017:2015	Information technology - Security techniques - Code of practice for information security controls
ISO 27018:2019	Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

xMatters has successfully completed a **SOC 2 Type II** examination for infrastructure and operations of our platform. xMatters also has **SOC 3 report**, which is a publicly shareable version of xMatters SOC 2 report.

Our security framework includes:

- Policies, procedures and controls
- Asset Management
- Risk Management
- Access Management
- Organizational Security
- Physical Security
- Cryptography
- Operations security
- Supplier security
- Business continuity
- Compliance

Security is the responsibility of all xMatters personnel. The entire team is regularly trained, and our systems and processes are audited at planned intervals. The Privacy Officer and the Information Assurance Manager define and maintain the security portfolio up-to-date. The ISMS Steering Committee reviews the entire program and controls on a regular basis during the Management Review Meetings.

Organizational Security

Each employee goes through a comprehensive security training, and awareness campaigns and meetings happen regularly.

Background Check

Prior to employment, potential candidates undergo interviews for suitability into the vacant role and a full spectrum background check. Upon employment, the candidate must read, sign, and adhere to a series of documents outlining their responsibilities for information security.

Termination of Employment

Terminated employees are removed from all systems. All access to management systems, hardware, tools and SaaS platform is revoked immediately. All assets must be returned to the company.

Acceptable Use Policy (AUP)

xMatters AUP is a set of rules that must be followed by all xMatters employees. The document focuses on the handling procedures of any asset – including data, hardware, and information systems (software) – to produce security-conscious operations for minimizing risk to people, processes, technology, and environments.

Security Awareness

An information security competence and awareness program is in place so employees can perform their functions in an secure manner.

Endpoint Security

All workstations at xMatters are configured by Corporate IT Director (CorpIT) to comply with our standards for security. These standards require all workstations to be properly configured and updated, and to be tracked and monitored by a secure endpoint management solution

Mobile devices used to engage in company business are required to be enrolled in the appropriate mobile device management system and to meet CorpIT security standards.

Access Control

Users are only provided with access to the network, systems, applications, and network services that they have been specifically authorized to use. Access to the system is audited semi-annually, logged, and verified.

To further reduce the risk of unauthorized access to data, xMatters Access Control model is based on Mandatory Access Control (MAC) using Role Based Access Control (RBAC) to create separation of state. There is continuous monitoring at the application and infrastructure level with all monitoring data sent to a Security Information and Event Management (SIEM) system. Principles of least privilege are enforced.

xMatters employs multi-factor authentication for all access to systems with client data. Whenever possible, xMatters uses private keys for authentication, in addition to the multi-factor authentication on a separate device. Clients can also use Federated Access Control; xMatters uses Security Assertion Markup Language (SAML) version 2.0 protocol for Identity Provider (IDP) Single Sign-On (SSO).

All employees are required to use an approved password manager. Password managers generate, store, and enter unique and complex passwords to avoid password reuse, phishing, and other password-related risks. To manage access to these accounts, xMatters uses LastPass Enterprise for authentication.

Monitoring and logging

xMatters access control and continuous monitoring logs all database access and ships the logs to a centralized SEIM system. Administrative access, use of privileged commands, and system calls on all servers are logged and retained.

Log information is protected against tampering and unauthorized access. System administrator and system operator activities are logged, and access/change actions can be reviewed.

For corporate data, xMatters uses Intelligent Hub (Formerly VMWare AirWatch), for monitoring policy compliance.

Malware Protection

Servers and endpoint devices such as laptops and desktops are protected and monitored from malwares, malicious and unsafe codes or applications by deploying a set of protection tools.

Physical Security

Access to the office, computer room, and work area containing sensitive information will be physically restricted to limit access to only authorized personnel. Employees use access cards for entering the offices and maintain a visitor log. Physical Security Audits are conducted annually. There are surveillance cameras and security in place to monitor the buildings.

Supplier Management

xMatters uses third-party sub-processors to provide infrastructure services, and to help us provide notifications and other associated services. Prior to engaging any third-party sub-processor, xMatters Information Assurance Team performs diligence to evaluate their privacy, security, and confidentiality practices, and executes a non-disclosure agreement implementing its applicable confidentiality obligations. The assessment process is repeated annually.

External Validation

Audits

xMatters is continuously monitoring, auditing, and improving the effectiveness of our security controls and compliance to privacy regulations. These activities are regularly performed by independent external assessors, authorized certification suppliers, and by xMatters internal IA Team. Audit results are discussed during management review meetings and all findings are tracked to resolution.

Vulnerability and Penetration testing

xMatters engages independent vendors to conduct application and infrastructure-level vulnerability scanning and penetration testing on the SaaS platform. All findings are logged into a database, risks are identified, assessed, and treated until residual risk comes down to the lowest acceptable level. Results of vulnerability scans and risk assessments are available to users upon request.

Client Data Protection

Data as an asset (Classification and Handling)

At xMatters, data is treated as a valuable asset. Information assets of the organization will be classified based on their relative business value, legal requirements and impact due to loss of confidentiality, availability and integrity of the information asset. The level of security will be identified based on the information classification performed.

Customer data is classified at the highest level.

Data encryption

- **Data in Transit**: xMatters' cryptography controls use Hyper-Text Transfer Protocol Secure (HTTPS) over Transport Layer Security (TLS) version 1.2 and higher using 2048 bit key length, and Internet Protocol Secure (IPSec).
- **Data at Rest**: xMatters uses Data at Rest Encryption using GCP Key Management Service (KMS). All data is encrypted using 256-bit Advanced Encryption Standard (AES-256), with each encryption key is itself encrypted with a regularly rotated set of master keys. xMatters is the only entity that possess the keys for the Data at Rest Cryptographic Controls within GCP and therefore Google does not have access to the data. Each client database protected using schema separation.

Data Center Security

xMatters SaaS is hosted on Google Cloud Platform. GCP safety and security policies are also applicable to you, our customer. GCP data center operations comply with a set of standards and regulations including ISO 27001, ISO 27017, ISO 27018, SOC 1/2/3, PCI DDS, and CSA Star, among others.

For more information about GCP certifications and compliance, click here.

GCP Security Whitepaper can be found here.

Data Hosting

xMatters SaaS systems resides in Google Cloud Platform (GCP). The GCP IaaS is a very robust, redundant and fault tolerant network infrastructure that provides many privacy and security features that are in alignment and certified against national and international standards and frameworks.

Google provides additional information here.

xMatters cloud-based SaaS operates within different economic regions with data centers located at:

- European Union: London (europe-west2) and Germany (europe-west3).
- Asia-Pacific: Sydney, Australia (australia-southeast1) and Singapore (asia-southeast1).
- North America: Moncks Corner, South Carolina (us-east1) and Council Bluffs, Iowa (us-central1).

Data Deletion

Customer data is stored for as long as it is needed to meet xMatters operational needs, together with contractual legal and regulatory requirements. Data is retained for the duration of the contract or unless indicated within the Contract/Master Service Agreement (MSA). Data destruction and sanitization is conducted in alignment with the National Institute of Standards and Technology (NIST) Special Publication 800 – 88: Guidelines for Media Sanitization.

In the event of contract termination or deletion request client data is purged within 60 days, from both the primary and secondary Datacenters. In Google Cloud Storage, customer data is deleted through cryptographic erasure. This is an industry standard technique that renders data unreadable by deleting the encryption keys needed to decrypt that data.

Compliance

xMatters complies with applicable legal, regulatory and contract requirements as well as industry best practices. There is a comprehensive Privacy Program in place and annual audits are performed against regulatory requirements.

Cryptographic controls are used in compliance with all relevant agreements, laws, and regulations. Regular technical compliance reviews, including penetration testing and IT health checks of all information systems, are taken to ensure continued compliance.

Risk Management

xMatters has a Risk Management Procedure in place to identify, assess and treat risks depending on the level of impact and likelihood. After treatment, all risks are re-assessed for residual risk evaluation. Risks are only accepted when they reach the lowest level and no longer represent threats to xMatters system and data assets.

Incident Management

xMatters has an established procedure for responding to potential security incidents. All security incidents are managed by following the non-conformity treatment process:

- Immediate action
- Root-cause analysis and incident classification (based on severity)
- Corrective action
- Preventive action

All process is documented and updated annually. Lessons learned are kept for future reference.

In the event of an incident, affected customers will be informed by our Technical Support Team or Customer Success Manager.

Business Continuity and Disaster Recovery

Continuity management is a risk based approach to managing risks/issues that can cause interruption/disruption to business operations or service delivery operations. xMatters manages these risks by determining the most common causes if interruption/disruption and have prepared plans for treatment of these issues.

Within xMatters, the specific roles are identified in relation to continuity management endeavors. Each role has a defined responsibility.

xMatters Business continuity plans are effectively implemented by:

- Having all stakeholders briefed on the contents of the BCP and aware of their individual responsibilities;
- GCP to be tested and audit results discussed during Management Meetings; and,
- Failover tests updated annually.

Datacenter Disaster Recovery Process

xMatters operates in three global economic areas (North America , Europe-Middle East-Africa, Asia Pacific-Japan) residing in two GCP data centers in each region. The data centers are paired in each region to provide fault tolerance and redundancy at the data center level of operations. Client data is backed up between two data centers within the same economic region, with one data center providing services and the second data center providing standby services, in the event the primary site becomes unavailable. Should a single data center within an economic region become completely unavailable, all services will be transferred to the secondary data center

Recovery Time Objective & Recovery Point Objective

xMatters Recovery Time Objective is committed to the Service Level Agreements. Services delivered from CorpIT to internal-facing employees must be recovered within 24 hours. Services delivered from cloud-based software to external-facing clients must be recovered within 30 minutes.

xMatters Recovery Point Objective (RPO) is dependent on multiple factors and when delivered from SaaS: deliveries to external-facing clients must be recovered to a point within 24 hours. The 24-hour value is based on conducting backups of the supplied client data within each data center. NOTE: Client-

provided data is not backed up to removable media or removed from the data centers for back up purposes.