PRO-33: FINRA RULES: CYBERSECURITY ASSESSMENT

PROGRAM SUMMARY

2020/03/10

Created with **StandardFusion**. Copyright ©2020 Fireloft Inc.

This product includes standards copyrighted by the American Institute of Certified Public Accountants. All rights reserved. Portions of the ISO Standard have been reproduced with permission from the Standards Council of Canada. No further reproduction or distribution of this copy is permitted by electronic transmission or any other means. Portions of this product are provided courtesy of PCI Security Standards Council, LLC ("PCI SSC"). © 2006-2015 PCI Security Standards Council, LLC. All rights reserved. PCI SSC does not endorse this product, its provider or the methods, procedures, statements, views, opinions or advice contained herein. All references to documents, materials or portions thereof made available by PCI SSC ("PCI Materials") should be read as qualified by the actual PCI Materials. For questions regarding PCI Materials, please contact PCI SSC through its web site at https://www.pcisecuritystandards.org.

Effective From	2020/03/01	**Standards**	Finra Rules: Cybersecurity Assessment
Effective To	2022/03/31		
Report Date	2020/03/10		

Description

Financial Industry Regulatory Authority, Inc. (FINRA) is a private corporation that acts as a self-regulatory organization (SRO). The Financial Industry Regulatory Authority is the largest independent regulator for all securities firms doing business in the United States. FINRA's mission is to protect investors by making sure the United States securities industry operates fairly and honestly. FINRA oversees about 4,250 brokerage firms, about 162,155 branch offices and approximately 629,525 registered securities representatives and suppliers.

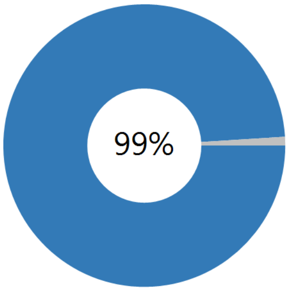
Scope

FINRA rules create a framework to check if suppliers have cybersecurity policies and procedures in place, as well as the proofs that these vendors are able to uphold them. With FINRA's increased focus on cybersecurity, xMatters is willing to take a proactive approach to satisfy regulators and financial institutions as clients.

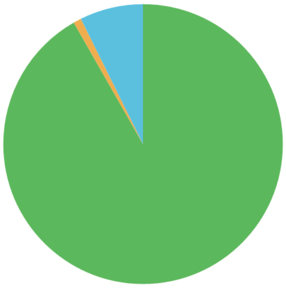
Notes

More information about Finra: www.finra.org.

Overall Progress



Implementation Status



100	Implemented
1	Partially Implemented
0	Not Implemented
8	Excluded

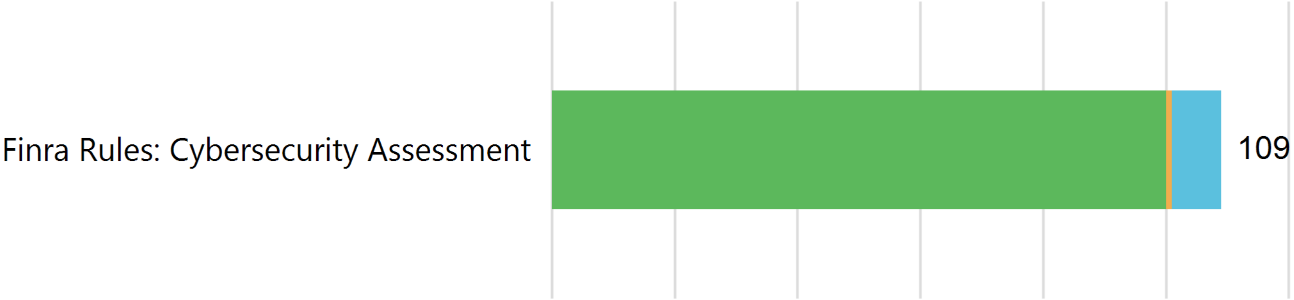
Total Controls/Policies

41

Number of Requirements

109

Requirements Per Standard



Requirement	Status	Owner
FINRA RULES: CYBERSECURITY ASSESSMENT		
PART 1: Cybersecurity Governance		

1.0 Cybersecurity Governance Implemented

1.A Chief Information Security Officer or Equivalent

Notes

xMatters has a Data Privacy Officer that oversees privacy and security process and ensures accountability.

1.0 Cybersecurity Governance Implemented

1.B Cybersecurity Governance Committee (CGC)

Satisfied By

- **Control:** Steering Committee

Notes

The ISMS (Information Security Management System) Steering Committee reviews the entire program and controls on a regular basis during the Management Review Meetings.

https://www.xmatters.com/trust/security/

1.0 Cybersecurity Governance Implemented

1.C Documented Cybersecurity Roles/Responsibilities

Satisfied By

- **Control:** ISMS Roles and Responsibilities

Notes

Management commitment to Information Security objectives and well-established roles and responsibilities.

https://www.xmatters.com/trust/security/

1.0 Cybersecurity Governance **Implemented**

1.D Documented Cybersecurity Risk Profile

Satisfied By

- **Policy:** P-11: Vulnerability Management Process (A1261)

Notes

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 processes are documented and updated annually. Lessons learned are kept for future reference.

https://www.xmatters.com/trust/security/risk-management/

1.0 Cybersecurity Governance **Implemented**

1.E Documented Cybersecurity Program

Satisfied By

- **Policy:** P-3: Information Security Code of Practice

Notes

Documented and monitored processes for incident management, data breach, risk assessment, nonconformities to the ISMS, and corrective action.

1.0 Cybersecurity Governance **Implemented**

1.F Risk Management Models (ISO/NIST/SANS 20)

Relates To

- **Program:** PRO-1: ISO 27001:2013

Satisfied By

- **Policy:** P-14: Risk Assessment (SOP 612)

Notes

Data Security: Our security practices and controls are aligned with the highest internationally recognized standards, such as ISO 27001 and NIST.

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.

https://www.xmatters.com/trust/security/risk-management/

1.2 Metrics and Thresholds **Implemented**

2.A Defined Implementation Metrics

Satisfied By

- **Policy:** P-20: Monitoring & Measuring (SOP 101)

Notes

Security policies, procedures and technical controls enable and effectively support the information security management and information security initiatives of XMatters.

xMatters Information Assurance Team has establish metrics that provide evidence about the transformation of information security policies into action and of their performance. The purpose of this procedure is to establish metrics in order to assist xMatters Management in ascertaining the extent to which the policies, procedures and controls are functioning effectively and whether or not the desired performance objectives are being achieved.

1.2 Metrics and Thresholds **Implemented**

2.B Defined Effectiveness/Efficiency Metrics

Satisfied By

- **Policy:** P-20: Monitoring & Measuring (SOP 101)

Notes

Controls and metrics are reassessed periodically and evaluated based on the Maturity Model (PMM: Project Maturity Model)

The procedure for monitoring and measurement shall determine the maturity level and effectiveness for each one of the ISMS controls.

1.2 Metrics and Thresholds **Implemented**

2.C Defined Impact Metrics

Notes

1.2 Metrics and Thresholds **Implemented**

2.D Defined Thresholds for Targeted Performance

Satisfied By

- **Policy:** P-1: Information Security Objectives (Doc 62)

Notes

PART 2: Cybersecurity Risk Assessment

2.1 Asset Inventory of Critical Assets **Implemented**

1.A Inventory All Asset Types

Satisfied By

- **Control:** C-27: Inventory of Assets

Notes

Keep an up-to-date data inventory. Our centralized GRC system streamlines the development of a mature and comprehensive data inventory and map. Customer information is treated as an asset and is an essential component of our inventory of assets.

2.1 Asset Inventory of Critical Assets **Implemented**

1.B Identify Critical Assets

Satisfied By

- **Control:** C-27: Inventory of Assets

Notes

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.

2.1 Asset Inventory of Critical Assets **Implemented**

1.C Identify Regulated Assets (eg: PII)

Relates To

- **Asset:** Client PII

Notes

https://www.xmatters.com/trust/privacy/privacy-notice/

2.1 Asset Inventory of Critical Assets **Implemented**

1.D Map Access to Assets (Firm Practices)

Satisfied By

- **Control:** C-29: Data Map

Notes

2.1 Asset Inventory of Critical Assets **Implemented**

1.E Evaluate Potential Resulting Damages

Satisfied By

- **Policy:** P-18: Breach response Process

Notes

We have a process in place to handle privacy breaches that involves, but is not limited to, report the breach, contain the breach and assess the extent and Impact of the Privacy Breach.

https://www.xmatters.com/trust/privacy/privacy-notice/

2.2 Risk Assessment Program and Governance **Implemented**

2.A Identify and Document Asset Vulnerabilities

Satisfied By

- **Control:** C-27: Inventory of Assets
- **Policy:** P-14: Risk Assessment (SOP 612)

Notes

A central risk management software connects threats to assets and, through a documented Risk Assessment Procedure, xMatters can track, remediate and control risks. Historical records and recent findings are analyzed during Risk Management Meetings.

https://www.xmatters.com/trust/privacy/ccpa/

2.2 Risk Assessment Program and Governance **Implemented**

2.B Document Threat Intelligence from Forums

Satisfied By

- **Control:** C-30: List of Legal, Regulatory, Contractual and Other Requirements (A1811)
- **Control:** C-26: Special Groups List (A614)

Notes

2.2 Risk Assessment Program and Governance **Implemented**

2.C Identify External Threat Actors

Satisfied By

- **Policy:** P-11: Vulnerability Management Process (A1261)
- **Policy:** P-14: Risk Assessment (SOP 612)
- **Policy:** P-13: Business Impact Analysis (A1713)

Notes

xMatters Business Impact Analysis (BIA) has the objective to identify and evaluate the risks and issues that may arise from natural and human (external) initiated events on xMatters operations.

2.2 Risk Assessment Program and Governance **Implemented**

2.D Identify Internal Threat Actors

Satisfied By

- **Policy:** P-4: Acceptable Use Policy

Notes

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.

2.2 Risk Assessment Program and Governance **Implemented**

2.E Identify Likely Cyber Attack Vectors

Satisfied By

- **Policy:** P-11: Vulnerability Management Process (A1261)

Notes

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.

2.2 Risk Assessment Program and Governance **Implemented**

2.F Identify and Prioritize Risk Responses

Satisfied By

- **Policy:** P-14: Risk Assessment (SOP 612)

Notes

https://www.xmatters.com/trust/security/risk-management/

2.2 Risk Assessment Program and Governance **Implemented**

2.G Document Past Cyber Incidents

Notes

A central risk management software connects threats to assets and, through a documented Risk Assessment Procedure, xMatters can track, remediate and control risks. Historical records and recent findings are analyzed during Risk Management Meetings.

2.2 Risk Assessment Program and Governance **Implemented**

2.H Risk Assessment Scoring System (CVSS)

Satisfied By

- **Policy:** P-14: Risk Assessment (SOP 612)

Notes

2.3 Periodic Cybersecurity Vulnerability Assessment **Implemented**

3.A Assessment Details (Who/Date)

Satisfied By

- **Policy:** P-11: Vulnerability Management Process (A1261)

Notes

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.

2.3 Periodic Cybersecurity Vulnerability Assessment **Implemented**

3.B Describe High to Critical Risks

Notes

2.3 Periodic Cybersecurity Vulnerability Assessment **Implemented**

3.C Penetration Testing Details (Results/Date)

Satisfied By

- **Policy:** P-25: Penetration Test (Veracode)

Notes

2.4 Periodic Physical Vulnerability Assessment **Implemented**

4.A Assessment Details (Who/Date)

Satisfied By

- **Control:** C-8: Office Physical Security Assessment Report (A111)
- **Control:** GCP Physical security perimeter (A1111)

Notes

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.

2.4 Periodic Physical Vulnerability Assessment **Implemented**

4.B Describe High to Critical Risks

Notes

2.5 Test Environment for New Software/Applications **Implemented**

5.A Test/Dev for New Software

Satisfied By

- **Control:** Systems Development Life Cycle (SDLC)

Notes

Production and testing environment are segregated.

2.5 Test Environment for New Software/Applications **Implemented**

5.B Test/Dev for Web Application

Notes

PART 3: Technical Controls

3.1 Defense in Depth Models (NIST/ISO) and Strategy **Implemented**

Satisfied By

- **Policy:** P-2: ISMS Manual
- **Policy:** P-3: Information Security Code of Practice

Notes

The xMatters security framework is governed by ISO/IEC 27001:2013 Information Security Standard and uses the comprehensive set of policies, processes, and controls for standardized treatment of data. All controls are centrally monitored and assessed for quality assurance. xMatters has a constantly improving security program in place with semi-annual internal audits conducted by an independent third party, and an external annual certification audit performed by an accredited organization.

https://www.xmatters.com/trust/security/

3.2 Identity and Access Management **Implemented**

2.A Documented Identity and Access Management Policy

Satisfied By

- **Policy:** P-23: Access Control (A91)

Notes

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.

3.2 Identity and Access Management **Implemented**

2.B Policy of Least Privilege Policy

Satisfied By

- **Policy:** P-23: Access Control (A91)

3.2 Identity and Access Management **Implemented**

2.C Separation of Duties Policy

Satisfied By

- **Policy:** P-23: Access Control (A91)

Notes

To further reduce the risk of unauthorized access to data, xMatters Access Control model is based on role based access control to create separation of state. There is continuous monitoring at the application and infrastructure level with all monitoring data sent to an event management system. Principles of least privilege are enforced.

https://www.xmatters.com/trust/security/organizational-security/

3.2 Identity and Access Management **Implemented**

2.D Entitlement Transparency (Documented)

Satisfied By

- **Control:** C-32: Role Base Access Control (RBAC)

3.2 Identity and Access Management **Implemented**

2.E Documented Authorization Scheme

Satisfied By

- **Policy:** P-8: Project Management and Change Management (A1212)
- **Control:** ISMS Roles and Responsibilities

Notes

3.2 Identity and Access Management **Implemented**

2.F Mechanism to Provision Entitlement

Satisfied By

- **Control:** Onboarding Checklist

Notes

Human Resources and Corporate IT follow a document to provision entitlement.

3.2 Identity and Access Management **Implemented**

2.G Mechanism to Monitor Use and Access Review

Satisfied By

- **Control:** C-14: A91 - Access Control Audits

Notes

3.2 Identity and Access Management **Implemented**

2.H Mechanism to Update Entitlement

Notes

xMatters has a document process applicable to change of employment.

3.2 Identity and Access Management **Implemented**

2.I Mechanism to Terminate Access

Satisfied By

- **Control:** Offboarding Checklist

Notes

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.

https://www.xmatters.com/trust/security/organizational-security/

3.2 Identity and Access Management **Implemented**

2.J Policy of Third-Party Access

Satisfied By

- **Policy:** P-30: Supplier Assessment and Monitoring (SOP A15)

Notes

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.

https://www.xmatters.com/trust/security/supplier-management/

3.3 Use of Data Encryption **Implemented**

3.A Encryption Mechanism for Data at Rest

Satisfied By

- **Control:** C-33: Cryptographic Controls (A101)

Notes

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.

https://www.xmatters.com/trust/security/data-encryption/

3.3 Use of Data Encryption **Implemented**

3.B Encryption Mechanism for Data in Transit (HTTP/VPN)

Satisfied By

- **Control:** C-33: Cryptographic Controls (A101)

Notes

xMatters' cryptography controls use Hyper-Text Transfer Protocol Secure (HTTPS) over Transport Layer Security (TLS) version 1.2 using 2048 bit key length, and Internet Protocol Secure (IPSec).

https://www.xmatters.com/trust/security/data-encryption/

3.4 Penetration Testing **Implemented**

4.A Assessment Details (Who/Date)

Notes

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.

https://www.xmatters.com/trust/security/assurance-process/

3.4 Penetration Testing **Implemented**

4.B Describe High to Critical Risks

Notes

3.4 Penetration Testing **Implemented**

4.C Penetration Testing Details (Results/Date)

Notes

PART 4: Incident Response

4.1 Incident Response **Implemented**

1.A Documented Incident Response Protocol

Satisfied By

- **Policy:** P-17: Nonconformity and Corrective Action (SOP 101)

Notes

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 processes are 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.

https://www.xmatters.com/trust/security/risk-management/

4.1 Incident Response **Implemented**

1.B Documented Team of First Responders

Notes

4.1 Incident Response **Implemented**

1.C Documented Notification Process (FINRA Rule 4530(b))

Satisfied By

- **Policy:** P-18: Breach response Process

Notes

We have a process in place to handle privacy breaches that involves, but is not limited to, report the breach, contain the breach and assess the extent and Impact of the Privacy Breach.

In the case of a privacy breach, we will, not later than 72 hours after having become aware of it, notify the data breach to the supervisory authority. When the personal data breach is likely to result in a high risk to your rights, we will communicate the personal data breach to you without undue delay.

xMatters Privacy Officer is responsible for maintaining and applying this procedure.

https://www.xmatters.com/trust/privacy/privacy-notice/

4.1 Incident Response **Implemented**

1.D Procedures to Determine the Scope of a Breach

Notes

4.1 Incident Response **Implemented**

1.E Procedures to Remediate Breach

Notes

4.1 Incident Response **Implemented**

1.F Periodic Fire Drills to Test IR Protocols and Teams

Notes

4.1 Incident Response **Implemented**

1.G Procedures to Make Clients Whole

Relates To

- **Control:** C-9: Communication Matrix

Notes

PART 5: Vendor Management

5.1 Cybersecurity Risk Assessment **Implemented**

1.A Physical Access Controls

Satisfied By

- **Policy:** Security at xMatters

Notes

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

https://www.xmatters.com/trust/security/organizational-security/

5.1 Cybersecurity Risk Assessment **Implemented**

1.B Network Access Controls

Satisfied By

- **Policy:** P-23: Access Control (A91)

Notes

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.

https://www.xmatters.com/trust/security/organizational-security/

5.1 Cybersecurity Risk Assessment **Implemented**

1.C Restricted Access/Least Privilege Access Controls

Satisfied By

- **Policy:** P-23: Access Control (A91)
- **Control:** C-32: Role Base Access Control (RBAC)

Notes

To further reduce the risk of unauthorized access to data, xMatters Access Control model is based on role based access control to create separation of state. There is continuous monitoring at the application and infrastructure level with all monitoring data sent to an event management system. Principles of least privilege are enforced.

https://www.xmatters.com/trust/security/organizational-security/

5.1 Cybersecurity Risk Assessment **Implemented**

1.D Test/Dev Environment for New Software/Apps

Satisfied By

- **Control:** Systems Development Life Cycle (SDLC)

Notes

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.

https://www.xmatters.com/trust/security/assurance-process/

5.1 Cybersecurity Risk Assessment **Implemented**

1.E Controlled Baseline System Configurations

Notes

5.1 Cybersecurity Risk Assessment **Implemented**

1.F Controlled System Maintenance (Patching)

Satisfied By

- **Policy:** P-11: Vulnerability Management Process (A1261)

Notes

5.1 Cybersecurity Risk Assessment **Implemented**

1.G Controlled Removal/Disposal Assets

Satisfied By

- **Control:** C-19: xMatters Deletion Process (GCP)
- **Policy:** P-7: Disposal of Media Process (A832)

Notes

Data is retained for the duration of the contract or unless indicated within the 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.

https://www.xmatters.com/trust/security/data-deletion/

5.1 Cybersecurity Risk Assessment **Implemented**

1.H Policies and Controls for Mobile/Removable Devices

Satisfied By

- **Control:** C-11: Device Management

Notes

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, including endpoint protector.

https://www.xmatters.com/trust/security/organizational-security/

5.1 Cybersecurity Risk Assessment **Implemented**

1.I Documented Policies/Controls for Data Disposal

Satisfied By

- **Control:** C-19: xMatters Deletion Process (GCP)

Notes

Data is retained for the duration of the contract or unless indicated within the 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.

https://www.xmatters.com/trust/security/data-deletion/

5.1 Cybersecurity Risk Assessment **Implemented**

1.J Testing of Back-up Systems

Satisfied By

- **Policy:** Disaster Recovery Plan (A1122)
- **Control:** C-34: Disaster Recovery Tests (A1122)

Notes

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 .

https://www.xmatters.com/trust/security/business-continuity-disaster-recovery/

5.1 Cybersecurity Risk Assessment **Implemented**

1.I Periodic Compliance Audits

Relates To

- **Audit:** AUD-7: GDPR, CCPA, PIPEDA, APP
- **Audit:** AUD-6: HIPAA

Satisfied By

- **Policy:** Internal Audit (SOP 92)

Notes

Security Standards

xMatters has a constantly improving security program (ISO 27001 / SOC 2) in place with semi-annual internal audits conducted by an independent third party, and an external annual certification audit performed by an accredited organization.

https://www.xmatters.com/trust/security/

Privacy Assurance

The xMatters Privacy Program is designed to assure the highest possible levels of privacy protection to our customers. We have developed and implemented transparent, comprehensive processes as part of our commitment to the responsible use of information.

Our privacy program is fully compliant with the following industry standards, and meets or exceeds all applicable requirements from Privacy Regulations.

The xMatters Privacy Program is reviewed by an independent, reputable third party on an annual basis. The xMatters Information Assurance team is responsible for managing and updating the privacy policy and procedures.

https://www.xmatters.com/trust/privacy/

5.2 Contractual Provisions **Implemented**

2.A Non-Disclosure/Confidentiality Agreements

Satisfied By

- **Control:** MNDA
- **Control:** C-15: Visitor NDA
- **Control:** C-49: Employee NDA

Notes

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.

https://www.xmatters.com/trust/security/supplier-management/

5.2 Contractual Provisions **Implemented**

2.B Data Storage/Retention/Delivery

Notes

https://www.xmatters.com/trust/privacy/privacy-notice/

5.2 Contractual Provisions **Implemented**

2.C Breach Notification Responsibilities

Notes

https://www.xmatters.com/trust/privacy/privacy-notice/

5.2 Contractual Provisions **Implemented**

2.D Right-to-Audit

Satisfied By

- **Control:** MSA (Master Service Agreement)

Notes

5.2 Contractual Provisions **Implemented**

2.E Vendor Employee Access Limitations

Satisfied By

- **Policy:** P-30: Supplier Assessment and Monitoring (SOP A15)

5.2 Contractual Provisions **Implemented**

2.F Use of Subcontractors

Satisfied By

- **Policy:** P-30: Supplier Assessment and Monitoring (SOP A15)

Notes

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.

To obtain a complete list of xMatters sub-processors, contact security@xmatters.com.

5.2 Contractual Provisions **Implemented**

2.G Obligations Upon Termination

Satisfied By

- **Control:** MSA (Master Service Agreement)

Notes

5.3 Segregation/Limitations to Third-Party Network Access **Excluded**

Notes

5.4 Third-Party Remote Maintenance Policies and Procedures **Excluded**

5.5 Incident Response Protocols **Implemented**

5.A Documented Incident Response Protocol

Satisfied By

- **Policy:** P-17: Nonconformity and Corrective Action (SOP 101)

Notes

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 processes are 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.

https://www.xmatters.com/trust/security/risk-management/

5.5 Incident Response Protocols **Implemented**

5.B Documented Team of First Responders

Notes

5.5 Incident Response Protocols **Implemented**

5.C Documented Breach Reporting Decision Tree

Notes

5.5 Incident Response Protocols **Implemented**

5.D Procedures to Determine the Scope of a Breach

Notes

5.5 Incident Response Protocols **Implemented**

5.E Procedures to Remediate Breach

Satisfied By

- **Policy:** P-18: Breach response Process

Notes

5.5 Incident Response Protocols **Implemented**

5.F Periodic Fire Drills to Test IR Protocols and Teams

Notes

5.6 SSAE SOC II Security Audit and Report **Partially Implemented**

Relates To

- **Program:** PRO-28: SOC 2 Framework (Security/Availability)

Notes

xMatters has initiate engagement for SOC 2 Type II and the final audit/report is due in November 2020. In the meantime, an internal audit program was implemented for continuously monitoring, 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 Information Assurance Team.

PART 6: Staff Training

6.1 Training Planning **Implemented**

1.A Frequency and Milestone Triggers

Satisfied By

- **Policy:** Competence and Training (SOP 72)

Notes

We monitor a complete organizational framework to ensure that client data is always secure and each employee goes through a comprehensive security assessment and training.

https://www.xmatters.com/trust/security/organizational-security/

6.1 Training Planning **Implemented**

1.B Content and Content Updates

Satisfied By

- **Policy:** Competence and Training (SOP 72)

Notes

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

https://www.xmatters.com/trust/security/organizational-security/

6.1 Training Planning **Implemented**

1.C Development and Delivery Mechanisms

Relates To

- **Control:** Security Awareness and Training
- **Control:** C-24: Training Certificates

Satisfied By

- **Policy:** Competence and Training (SOP 72)

6.2 General Training Content **Implemented**

2.A Recognizing Threats

Notes

6.2 General Training Content **Implemented**

2.B Social Engineering Schemes and Phishing

6.2 General Training Content **Implemented**

2.C Handling Confidential Information

6.2 General Training Content **Implemented**

2.D Password Protection

6.2 General Training Content **Implemented**

2.E Escalation Policies

6.2 General Training Content **Implemented**

2.F Physical Security

6.2 General Training Content **Implemented**

2.G Mobile Security

6.3 IT/Management Training **Implemented**

3.A Application Lifecycles

6.3 IT/Management Training **Implemented**

3.B Application Security

6.3 IT/Management Training **Implemented**

3.C Privilege Management

6.3 IT/Management Training **Implemented**

3.D Emerging Technology

6.3 IT/Management Training **Implemented**

3.E Software Vulnerabilities

PART 7: Cyber Intelligence and Information Sharing

7.1 Intelligence and Information Sharing Planning **Implemented**

1.A Assign Responsibility for Cyber Intelligence

Satisfied By

- **Policy:** P-2: ISMS Manual
- **Policy:** P-3: Information Security Code of Practice

Notes

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.

https://www.xmatters.com/trust/security/

7.1 Intelligence and Information Sharing Planning **Implemented**

1.B Mechanism to Disseminate Threat Intelligence

Satisfied By

- **Control:** Trust Portal

Notes

7.1 Intelligence and Information Sharing Planning **Implemented**

1.C Identify Threat Intelligence Sources

Satisfied By

- **Policy:** P-11: Vulnerability Management Process (A1261)

Notes

7.1 Intelligence and Information Sharing Planning **Implemented**

1.D Identify and Participate in Information Sharing Organizations

Satisfied By

- **Control:** C-26: Special Groups List (A614)

7.2 Information Sharing Organizations and Resources **Excluded**

2.A MSSP or Managed Service/Software Vendor

7.2 Information Sharing Organizations and Resources **Excluded**

2.B FS-ISAC

7.2 Information Sharing Organizations and Resources **Excluded**

2.C US Computer Emergency Readiness Team (US-Cert)

7.2 Information Sharing Organizations and Resources **Excluded**

2.D FBI or InfraGard

7.2 Information Sharing Organizations and Resources **Excluded**

2.E National Cyber Forensics and Training Alliance (NCFTA)

7.2 Information Sharing Organizations and Resources **Excluded**

2.F Department of Homeland Security (DHS)

PART 8: Cyber Insurance

8.1 Cyber Liability Insurance **Implemented**

1.A Documented Policy and Carrier

Notes

xMatters maintains a Cyber Liability Policy with a consolidated carrier that covers: Aggregate Limit of Liability for All Damages, Claim Expenses, Privacy Event Expenses, Extortion Payments, Privacy Regulation Investigation Expenses, First Party Loss under all Coverages, among others.

8.1 Cyber Liability Insurance **Implemented**

1.B First-Party Loss Coverage

8.1 Cyber Liability Insurance **Implemented**

1.C Third-Party Loss/Professional Liability

8.1 Cyber Liability Insurance **Implemented**

1.D Identify and Participate in Information Sharing Organizations