Security Program and Policy

XTM Security Program and Policy

Version 2.22p: June 2024

Version 1.0: October 2013

Published by XTM Holdings Inc.

Table of contents

0. Versioning

Version	Date	Name	Description of changes
1.0	October 2013	-	First internal version.
2.22p	June 2024	Mateusz Pacek	Public version based on the internal 2.22 version.

1. Introduction

1.1 Security Program

The purpose of this Security Program is to document a formal security program that addresses the management of security and the controls employed within XTM Group. The structure of this document is aligned and consistent with ISO 27002:2013. This document was redacted to be a public version.

This Security Program comprises:

- A documented Information Security Policy, contained within this document that is formally approved by the Board and made public. The internal version of this policy is communicated to all appropriate personnel, and reviewed at least annually.
- Documented, clear assignment of responsibility and authority for security-related activities.
- Regular testing of key controls, systems and procedures of the Security Program by the management, on a regular basis, and by an independent third party (see annex for details) concerning information systems at least annually.

“Security Obligations” means those measures designed to protect data against accidental or unauthorised destruction or accidental loss, alteration, unauthorised disclosures or access and against all other unauthorised forms of processing.

XTM Group has clear Security Obligations towards its Customers.

1.2 ISO 27001 Certification

XTM Group is ISO 27001 certified. This document provides a summary of the XTM Group ISO 27001 Certified Security Documentation. Detailed information on specific topics is available in the XTM Group ISO 27001 Certified Security Documents, which are available on request.

1.3 Security Policy

The highest priority is given to keep XTM Group's Customer data secure and confidential. No access to Customer data is permitted, except in the case of resolving support issues at the Customer's request. No Customer data is ever held on any personal computers and/or removable media and Customer data is only ever copied as part of resolving a support related issue. All copied data is immediately deleted once the support issue has been successfully resolved.

1.4 Internal Audit

Periodic internal audits are carried out at least on an annual basis to measure compliance and effectiveness. All company employees are encouraged to participate in helping to manage the effectiveness and compliance of the Security Program and Policy.

1.5 Third Party Security Audits

XTM International undergoes an annual ISO 27001 certification audit by an ISO 27001 certified auditing organisation. The first audit was carried out in January 2019.

Independent third-party penetration testing of the XTM application is carried out on an annual basis by an independent third-party penetration testing specialist company. Penetration testing includes but is not limited to OWASP Top 10 Vulnerabilities. Each new version of XTM undergoes internal penetration testing as part of each new release.

1.6 Formal Procedures

All formal procedures are executed via an appropriate Jira issue in the XTM Jira system providing an evidence based approach.

2. Risk Assessment and Treatment

2.1 Purpose

To undertake regular information risk management for key aspects of the service in a rigorous and consistent manner using a structured methodology.

2.2 Risk Management

XTM Group maintains an information security management system (ISMS) risk assessment program that performs regular risk assessments, is evaluated formally once a month, and includes controls for risk identification, analysis, monitoring, reporting and corrective action.
Risks must be assessed in terms of:

1. The likelihood of a risk arising
2. The severity of the impact

2.3 Information Classification and Handling

All Customer information is treated as highly confidential, during receipt, creation, processing, in transit, in storage, and on backup media.

2.4 Security Risk Assessment

1.0 Purpose

To provide periodic information security risk assessments (RAs) for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

A 'Risk' is defined as those factors that could affect confidentiality, availability, and integrity of XTM Group's key information assets and systems. XTM Group is responsible for ensuring the integrity, confidentiality, and availability of critical information and computing assets of its Customers as well as its own data, while minimising the impact of security procedures and policies upon business productivity.

2.0 Scope

Risk Assessments can be conducted on any information system, to include applications, servers, and networks, and any process or

procedure by which these systems are administered and/or maintained.

3.0 Policy

The execution, development and implementation of remediation programs is the joint responsibility of the CTO and CEO. All Employees are expected to cooperate fully with any RA being conducted on systems for which they are held accountable. Employees are further expected to work with the InfoSec Risk Assessment Team in the development of a remediation plan.

2.5 Third Party Vendor Management

Third party vendors are a core part of the continuous risk assessment. Third party vendors must also supply a SLA on engagement which must include provisions for strict confidentiality of data held on behalf of XTM Group and its Customers.

Third Party Vendor Management includes the following ongoing risk areas which must be assessed regularly:

1. **Information Security/Data Privacy**
   Does the third party have insufficient experience & controls to protect the company's and Customer's information from unauthorised access, disclosure, modification, or destruction.
2. **Business Continuity**
   Does the third party have a Business Continuity Plan and can it maintain its services due to business disruption.
3. **Financial Viability**
   Is the third party sufficiently financially secure to continue to provide the services at acceptable levels.
4. **Physical Security**
   Does the third party lack the proper security to prevent unauthorised access to its facilities, equipment and resources to protect from damage or harm.
5. **Contract Compliance**
   Are the third party's products, services or systems consistent with XTM Group's policies and procedures, agreed contract levels, applicable law, regulations and ethical standards.

6. **Legal/Regulatory**
   Does the third party possess the necessary licenses to operate and the necessary expertise to enable the company to remain compliant with domestic and international law and regulations.

7. **4th Party Subcontractor**
   Does the third party contract out any part of its services to a 4th party. This can cause additional risk and must be assessed on the same basis as the third party itself.

3. Information Security Policies

3.1 Purpose

To provide management direction and support for developing and distribution of XTM Group's comprehensive approved information security policy to all individuals with access to Customer data.

3.2 Obligations

XTM Group will:

1. Act diligently when handling customer information.
2. Implement best practice in relation to information security based on the ISO 27002 standard and demonstrate accreditation with a recognized Information Security certification.
3. Possess a formal Information and IT Security Policy, as evidenced and detailed in this document, which is approved by management, available to all employees and any associated external parties.
4. Undertake security awareness training as part of its Information Security program
5. Demonstrate accreditation with a recognized Information Security certification ISO 27001.

4. Organisations of Information and IT Security

4.1 Purpose

Provide a top down management structure and mechanism for coordinating security activities and supporting the Information Security program/approach within the organisation.

4.2 Requirements

XTM Group will:

1. Ensure all Supplier personnel, Subcontractors and Consultants are given adequate training to meet the needs of providing the agreed Services to Customers.
2. Ensure that all of its employees, Consultants, Subcontractors and other individuals are aware of XTM Group confidentiality obligations as well as the accepted use of information, facilities and systems.
3. Be able to certify and attest at any given time the names of, and the contact information (such as telephone number and e-mail address) to, all of its employees, Consultants, Subcontractors and any other individuals working under the XTM International's responsibility.
4. XTM Group has assigned roles to ensure security standards are maintained.

5. Human Resources Policy

5.1 Purpose

Provide a top down management structure and mechanism for coordinating security activities and supporting the Information Security program/approach within the organisation.

5.2 Worker Responsibilities

XTM Group ensures that all employees, agents, and contractors (collectively "Workers") acknowledge their responsibility to: maintain the confidentiality of Customer Confidential Information; comply with XTM Group's internal information security and acceptable use requirements; and comply with the requirements herein.

All Workers are required to sign a declaration to this effect at the start of their employment and annually in January.

5.3 Personnel

XTM Group does not hire, retain or engage Workers who have been convicted of fraud, embezzlement, larceny, perjury, terrorism, or breach of trust or fiduciary duty to perform any responsibilities or functions in connection with handling Customer confidential information.

Background checks are conducted on all current or prospective workers who will handle Customer confidential information.

5.4 Security Awareness Training

XTM Group conducts security awareness training regarding XTM Group security requirements for all workers who will handle Customer confidential information.

XTM Group maintains records showing the names of Workers in attendance and date of each security awareness training. XTM Group also routinely reviews and updates its security awareness training on an annual basis. Training includes social engineered vulnerabilities such as phishing attacks etc.

The training is carried out using a Social Engineering platform - KnowBe4.com.

The platform is also used to perform an annual security assessment for all employees of XTM Group.

5.5 Clean Desk Policy

XTM Group operates a 'clean desk policy' requiring no paper documents to be left on Workers desks at the end of the working day.

5.6 Privacy

All Customer data must be treated with the highest level of security designation. The privacy of Customer data is paramount. Customer data can only be accessed at the Customer's behest.

5.7 Acceptable Use Policy

Use of the Internet including email by Workers is strictly for business use only and must comply with current legislation and must not be misused. Any activity connected to socially unacceptable behaviour as well as fraud will form grounds for disciplinary action up to and including termination of employment.

5.8 Enforcement

Any Worker found to have violated any requirements in this Security Program and Policy document may be subject to disciplinary action, up to and including termination of employment.

5.9 Dismissal

Any Worker found in violation of terms of employment, including security policies is liable to be dismissed. Serious violations may cause immediate dismissal and removal from XTM Group's premises.

On dismissal for any reason a Worker with access to confidential Customer data, confidential company data of any type, or XTM source code, will leave the company immediately and not work their notice period. XTM Group will pay the member of staff in lieu of their notice period, if applicable.

5.10 Termination of Employment

All Workers leaving the company have all of their electronic credentials revoked and all passes invalidated immediately on leaving the company. All keys and any company equipment is handed in to the immediate line manager.

6. Asset Management

6.1 Purpose

To document and agree confidentiality obligations for information and determine the appropriate level of protection that should be applied to prevent any unauthorised disclosure.

6.2 Asset Program

XTM Group maintains an Asset Management program comprising:

1. A comprehensive hardware and software inventory.
2. The assignment of assets to employees to insure the appropriate classification of information, determination of access restrictions, and access controls.
3. The requirement to delete all data from data storage devices upon reassignment of the device or disposal. A Jira admin task must be associated with each device to be wiped clean.
4. The authorised by a first line manager for the removal of equipment, information or software to any off-site location. The asset is subsequently logged and tracked.
5. All acquisitions, removal from the office and disposal of any IT asset must be accompanied by a formal Jira issue task and signed off by the appropriate manager.

7. Access Control

7.1 Purpose

To ensure that only authorised individuals are allowed to gain access to business applications, information systems, networks and computing devices, that individual accountability is assured and to provide authorised users with access privileges that are sufficient to enable them to perform their duties, but do not permit them to exceed their authority.

7.2 Access Authorization and Control

Access to Customer Confidential Information and Customer systems is only allowed for duly authorised roles. Access is regularly reviewed including offboarding and role changes.

7.3 Regulator Audits and Examinations

As permitted by United States Statute, XTM Group will provide United States based Customers with immediate written notice if a United States federal or state regulatory agency ("Regulator") requests a non-routine review, audit or other examination of the records and systems maintained by XTM Group ("Regulatory Audit") that support or contain Customer Confidential Information. XTM Group will fully cooperate with Customers and the Regulator(s) in the event of a Regulatory Audit.

7.4 Role Based Access Control (RBAC)

Access control to resources is enabled according to the individual user's role. The principle of least privilege (POLP) is used within XTM Group, limiting access rights for users to the bare minimum required to fulfil their function.

7.5 Segregation of Duties (SOD)

XTM Group implements a Segregation of Duties (SOD) approach of sustainable risk management and internal controls for a business. The principle of SOD is based on shared responsibilities of a key process that disperses the critical functions of that process to more than one person or department. Using the SOD approach in key processes, fraud and error risks are far more manageable.

7.6 Identity Management

Identity management for all Workers is managed via a centralised service. Unique usernames are required and two factor authentication used in order to log into internal networks and systems.

7.7 Access Rights

Access rights to all systems as well as processing facilities are withdrawn immediately on Workers termination of employment.

7.8 Cryptographic Controls

XTM Group has appropriate cryptographic controls that are applied to Customer Confidential Information in transit across or to networks for which XTM Group does not have management responsibilities, including those used for sending data to Customer Corporate network from XTM Group's network.

7.9 Logging Requirements

XTM Group collects audit logs and regularly reviews logs for anomalies. Significant security and system events, such as failed attempts to gain root privilege, changes to firewall rules, adding a new user etc. are logged to a central event log for review.

7.10 Password Policy

XTM Group adheres to the cyber security guidelines laid down by the UK National Cyber Security Centre;(https://www.ncsc.gov.uk/blog-post/problems-forcing-regular-password-expiry).

Users are required to change their password once a year. The formal requirements for passwords are managed by the Admin team in accordance with industry best practices.

8. Cryptography

8.1 Purpose

To protect the confidentiality, authenticity and/or integrity of information by proper and effective use of cryptography.

8.2 Obligations

XTM Group will:

1. Use suitable and agreed encryption techniques.
2. Whenever encryption is used XTM Group is responsible to ensure that key management in support of authorised encryption techniques is in place. The use of cryptography is supported with procedures and protocols for the generation, change, revocation, destruction, distribution, certification, storage, entry, use and archiving of cryptographic keys to ensure the protection of keys against modification and unauthorised disclosure.

9. Physical and Environmental Security

9.1 Purpose

To protect IT facilities equipment and services against malicious attack, accidental damage, natural hazards and unauthorised physical access thus ensuring critical equipment is available when required and prevent important services from being disrupted by loss or damage to equipment or facilities.

9.2 High Risk Security Zones

The high-risk zones for XTM Group are the development and support offices in Poznań and Kraków in Poland.

9.3 Handling of Customer data

All staff working with Customer data for support purposes can only access such data at the Customer's behest. Any data that needs to be reviewed and/or copied onto a local PC can only be copied to XTM Group PCs/laptops. All XTM Group development and support PCs/laptops have their local disk partitions encrypted.

Under no circumstances is it permissible to copy any Customer data onto Workers personal PCs, laptops or storage devices.

9.4 Data encryption at REST

Data at REST is encrypted in XTM if the appropriate system settings are made, as well as all disks used in the specific XTM instance. Data at REST is encrypted for the instances hosted on AWS (EBS encryption with AES-256 algorithm).

9.5 Two factor authentication

Access to all production servers as well as test and user acceptance servers managed by XTM Group staff must be by means of two factor authentication.

9.6 Support Utilities

XTM Group protects facilities containing Customer Confidential Information and other Customer information and systems from failures of power, telecommunications, water supply, sewage, heating, ventilation and air-conditioning.

10. Operations Security

10.1 Purpose

To protect critical and sensitive information handled by XTM Group.

10.2 Device Configuration Standards

All servers, routers and switches and any other programmable networking devices include security hardening procedures consistent with industry best practices.

10.3 Operating System and Operational Software Patch Management

XTM software development team members ,XTM systems admin team and XTM security team are tasked with constant monitoring for information regarding any vulnerabilities to operating system and utility software. Vulnerabilities are evaluated according to severity and appropriate patches are implemented as required.

10.4 Change Control

All change requests must be approved. No new software releases and patches are implemented without a Jira issue being raised. All source code is checked in to the Git software repository and a clean build of the system produced for testing through the continuous build process. All new software releases are tested by the test department. All software patches are only implemented by a duly authorised systems administrator.

10.5 Segregation of Duties

XTM Group segregates duties and areas of responsibility so that no one person has sole access to Customer Confidential Information or processes which could lead to unauthorised modification or misuse of Customer Confidential Information or assets.

10.6 Technical Architecture Management

XTM Group maintains a configuration management process to define, manage, and control the components of the service and technical infrastructure.

10.7 Intrusion Detection

XTM Group continually monitors systems and processes for security intrusions or violations and will notify Customers if suspicious conditions or activities are detected indicating an actual or potential security violation or intrusion.

10.8 Network Security

XTM Group ensures the following:

1. Network intrusion detection system (IDS)/ intrusion prevention sensors (IPS) alert events are logged and reviewed at least daily for necessary intervention.
2. IDS/IPS are updated at least daily and run the latest threat signatures or rules.
3. High-risk ports on externally-facing systems are monitored.
4. All Internet based network connections are logged and recorded in log files.
5. The appropriate firewalls are present and correctly configured and maintained.
6. All Inbound and outbound network service traffic that accesses Customer systems are encrypted.
7. All network and diagnostic ports are properly secured.
8. Policies, procedures and technical controls that prevent, detect and remove malicious code or covert channel attacks on XTM Group's information systems are in place.

10.9 Encrypted Authentication Credentials

XTM Group ensures that authentication credentials transmitted to network devices are encrypted in transit.

10.10 Secure Network Administration

Networks are adequately managed and controlled to protect from threats, and to maintain security for all applications and data on the network or in transit over the network. Technical controls and secure communication protocols are implemented to prohibit unrestricted connections to untrusted networks or publicly accessible servers.

Two factor authentication is mandated to access any servers managed by XTM Group for support purposes.

10.11 Virus Protection

XTM Group ensures a virus management program is in place and signature files are up-to-date for servers and workstations used to house or access Customer Confidential Information.

10.12 Physical Media

All physical media is securely wiped clean of all data prior to disposal.

10.13 Electronic Information in Transit

XTM Group protects information involved in Customer data that passes over public networks from unauthorised disclosure and modification.

10.14 Data Integrity

XTM International has appropriate testing and protection controls in place to protect the integrity of Customer information made available on publicly accessible systems from unauthorised modification.

10.15 Wireless Networks

XTM Group ensures the following:

1. Wireless network access is strictly prohibited from any XTM workstation/PC within the support and development offices.
2. A guest network is made available that is totally separate and not connected in any way to the internal Ethernet network within the support and development offices. A special wireless network is maintained for mobile application development.
3. That both encryption and strong authentication is required to connect to approved wireless access points.

10.16 Wireless Segregation

XTM Group segregates related groups of information services, users, and information systems on networks. A guest network will be provided for visitors that is physically segregated from the other XTM Group wireless mobile application development network.

XTM segregates servers in terms of designated usage. Servers are classified as:

Production, Testing and Development.

10.17 BYOD

The use of BYOD devices is prohibited. Only XTM Group owned and managed devices are allowed to be connected to the XTM CAT5 wired network in the XTM support and development office.

10.18 Mobile Devices

It is totally prohibited to store any company and/or Customer related information on any personal mobile device, be it a PC, smartphone or tablet. It is also totally prohibited to connect any personal mobile device to any of the production networks.

10.19 Remote working

All critical XTM resources can only be accessed via the XTM VPN network using 2 factor authentication. It is expressly prohibited to connect to the XTM VPN network using non-XTM personal computers.

11. Communications Security

11.1 Purpose

To protect critical and sensitive information when being transmitted.

11.2 Obligations

XTM Group will:

1. Ensure that Jira issues are always used as the formal policy to manage and communicate all relevant actions throughout the company.
2. Ensure networks operated by XTM Group are configured in a consistent, accurate manner with approved security settings applied to ensure that networks function as intended, are available when required and do not reveal unnecessary technical details.
3. Ensure that the environment used is monitored in such a way to provide for the detection and traceability of any events violating information and/or IT security.
4. Ensure that all data communication is performed in a secure manner.
5. Provide Customers with appropriate access information regarding support and relevant management contacts.

12 Information Systems Acquisition Development and Maintenance

12.1 Purpose

To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide Services over public networks.

12.2 Systems Development Security

XTM Group ensures that security is part of all information systems development and operations and will publish and adhere to internal secure coding methodologies based on application development security best practices.

12.3 Software Security Management

XTM Group information systems (including operating systems, infrastructure, business applications, off-the-shelf- products, services and user-developed applications) are designed to be in compliance with information security standards.

12.4 Network Diagrams

XTM Group develops, documents, and maintains physical and logical diagrams of networking devices and traffic.

12.5 Vulnerability Assessments

XTM Group will perform vulnerability assessments and network penetration testing annually on systems that Handle Customer Confidential Information.

12.6 Change Management

XTM Group reviews and tests changes to applications and operating systems prior to deployment to ensure there is no adverse effect on Customer Confidential Information or systems.

13 Information Security Incident Management

13.1 Purpose

To ensure a consistent and effective approach to the management of information security Incidents, including communication on security events and weaknesses.

13.2 Vulnerability Management

XTM Group maintains a Risk Register that is part of the XTM Group Risk Management Plan. The risk register addresses risk management in four key steps:

1. Identifying risks
2. Classifying each risk
3. Applying possible solutions to those risks
4. Monitoring and analysing the effectiveness of any subsequent steps taken to mitigate the risk.

13.3 Information Asset Handling

XTM Group holds and processes data for its Customers. All Customer data is treated with the utmost security. Only duly authorised personnel:

- Systems administrators
- First line support
- Second line support
- Third line support

Are allowed access to this data and only when requested by the Customers.

13.4 Incident Management Program

XTM Group has an information security incident management program (the “Program”) that addresses management of information security incidents and system weaknesses..

13.5 Chain of custody

XTM Group will maintain and secure any evidence regarding security incidents for chain of custody purposes. All evidence will be stored in a secure and tamper proof manner to present on request for legal purposes.

13.6 Incident Categories

The following categories of incident are defined:

1. Incident: an incident that required action to conform to the System Program and Policy document and ISO 27001 documentation requirements but did not result in any damage.
2. Important Incident: an incident that was discovered that did not result in any breach, such as notification of a vulnerability that was immediately patched.
3. Critical Incident: an incident that resulted in unauthorised access or damage to Customer data. Examples are:
    a. Security Events that compromises the integrity, confidentiality, or availability of an information asset.
    b. Data Breach which meets specific legal definitions regarding privacy data.

13.7 Incident Reporting

XTM Group will notify each Customer immediately if there is a Critical Incident involving the Customer's Confidential Information.

Notices are provided to the designated Customer contact(s).

13.8 Response

XTM Group partners with each Customer to respond to any security Incident affecting that Customer. Responses may include: identifying key partners, investigating the Incident, providing regular updates, determining notice obligations and identifying and executing remediation plans. Except as required by law, XTM Group will not notify affected parties, regulators or other third parties without prior consultation with the Customer.

13.9 Service Suspension

In the event of a Critical Incident and upon a Customer's request, XTM Group will cease, suspend, alter or modify, as reasonably necessary, the services it is performing if warranted by the severity of the incident.

14. GDPR

14.1 Purpose

To ensure Customers and workers personal data is stored and accessed in line with the General Data Protection Regulations (Data Protection Act 2018) which came into effect May 25th 2018.

14.2 Documents

XTM Group have in place the following documents which are in alignment with the principles under the Data Protection Act 2018;

- Data Retention Policy
- SARS Guidelines
- SARS Request Form
- Data Processing document
- Privacy Policy
- Website Privacy Policy
- Data Processing Agreement, and
- GDPR Compliance Statement.

14.3 Handling Personal Information

XTM Group is a data processor in relation to Customer and worker personal data. XTM Group's GDPR Compliance Statement sets out in detail its responsibilities as a data processor, which includes;

- Data Security
- Breach Notification
- Data Retention
- Accountability, and
- Privacy by design.

14.4 Processing Purpose

The processing purpose of XTM Group is to allow data controllers (users of XTM) to translate electronic documents from one language into another language or into multiple languages. XTM Group store and process personal information which the user enters into the TMS, which may include personal data such as;

- Name
- Email address
- Address
- Phone number
- Subject matter, and
- Other identifiers.

Processing of Customers personal data is always in accordance with the consent of that Customer. XTM Group may also process such data for legitimate interests or due to a legal or contractual requirement.

XTM Group has implemented appropriate technical and organisational measures designed to protect users and workers personal data from unauthorised or unlawful processing and against theft, alteration, destruction, accidental loss and disclosure. If XTM Group becomes aware of any accidental, unauthorised, altered or lost personal data that is processed by XTM Group in providing its services to the Customer, it will notify the Customer as soon as possible and provide a full description of the incident and subsequent updates.

XTM Group ensures all personnel have access to their personal data and have the right to delete, amend or request copies of such data at any time.

XTM Group shall assist with a Customers' request for assistance with the Customer's obligation to respond to an individuals' subject access request on the basis the Customer reimburses XTM Group for all costs incurred in such assistance.

Further information on XTM Group's responsibilities and processes relating to the Data Protection Act can be found in XTM' Groups 'GDPR Data Processing Addendum', 'GDPR Compliance Statement' and 'Privacy Policy'.

15. Business Continuity and Disaster Recovery

15.1 Purpose

To prepare for disturbances under normal circumstances and for states of emergency. Help to align business continuity goals, provide resilience against disruption and minimise impact to Customers in the event of a disaster or emergency.

15.2 Backups

All live production data is backed up and encrypted to a separate server in a physically separate data centre. Backups are conducted on a daily basis.

The XTM backup policy covers all production systems that XTM Group administers. Test, stage and development instances are not covered by this policy unless this is specifically requested by the Customer.

Performing consistent, regular backups of the full set of XTM data forms a vitally important part of the company's recovery strategy.

Backups are stored in secure encrypted form, which is a secure, durable, cloud storage service. It is designed to deliver 99.999999999% durability and provides comprehensive security and compliance capabilities that can help meet even the most stringent regulatory requirements.

All source code and build instructions are backed up daily and the backups are held encrypted in a physically separate data centre.

15.3 Business Continuity

XTM Group has multiple offices around the globe, with the principal ones located in London in the UK, Poznań and Kraków, Poland and Rochester, USA. No critical data infrastructure exists at any of these offices. XTM Group is fully capable of normal operations even if any of these offices are affected by a disaster. All operations can be continued by XTM Group personnel from home.

15.4 XTM Disaster recovery

The main XTM Cloud server cluster is located at the OVH facility in Northern France, while XTM Private Cloud instances are hosted in either AWS or OVH facilities in geographically designated regions according to customers' preferences. XTM disaster recovery comprises the following:

15.4.1 Process description

New hardware will be ordered and commissioned immediately. Operating system configuration and security patches will be applied. The basic logical software cluster will be created. The database software will be installed and the database will be configured. The XTM Cloud software will be installed and commissioned. The data will be restored from backup.

15.4.2 Recovery strategy

The recovery strategy depends on commissioning new servers and installing the operating system, installing the XTM software and recovering the data from backup. The recovery strategy is tested a few times a year. Recovery starts immediately upon notification of a major incident that requires recovery.

15.5 Serious Incident Management Committee

Any incident that potentially affects the well-being and goodwill of XTM Group concerning its Customers as well as the normal functioning of the company, requires the immediate invocation of the Serious Incident Management Committee. The committee will oversee and manage mitigating the effects of the incident.

16. OFAC

16.1 Statement

XTM International Inc. is a US registered entity and such entity does not engage in any trade or financial transactions with suppliers, customers, contractors, individuals or agents in the following countries;

- Cuba
- Iran
- Crimea Region of Ukraine
- North Korea
- Syria
- Belarus
- Burundi
- Central African Republic
- Democratic Republic of Congo
- Iraq
- Lebanon
- Libya
- Mali
- Nicaragua
- Russia
- Somalia
- South Sudan
- Venezuela
- Yemen
- Zimbabwe
- Cuba

XTM International Inc. upholds all sanctions and trade restrictions imposed by OFAC on individuals, entities, countries and organisations which have been found to have violated US export control laws, participated in proliferation activities, or been determined as a terrorist or been affiliated with terrorists. XTM International Inc does not trade with or make financial transactions to any supplier, customer, agent, contractor or individuals who are deemed by the OFAC as a risk to US foreign policy and/or national security.