Information Security Policy: General

Version V2.0 – Owner: R&C - IS Classification B-Internal

Version	**V2.0**
Owner	R&C
Created Date	17.07.2017
Approved by	CEO/CFO
Review Date	21.09.2022
Next Review Date	21.09.2022

Table of Contents

1. 1. Introduction

"Security Management" is the protection and preservation of our ***business assets*** so that we can:

- operate effectively as a business
- provide services to our customers in a reliable and secure manner
- maintain a safe and healthy working environment for our people and our visitors

For the purpose of this policy, our ***business assets*** include:

- The ***people*** we employ, or otherwise engage to work with us, including contractors and suppliers.
- The ***processes*** we use to run our business or deliver services to our customers.
- The ***hardware, software,*** and other ***tools*** *and* ***technology*** we use to support business operations and service delivery.
- The ***information*** and ***data sources*** M247 create, use or change (this includes data stored on computers and mobile devices, transmitted across networks, printed out or written on paper, sent by e-mail or fax, stored on tapes, disks, DVDs, CDs or memory devices, or spoken in conversation and over the telephone);
- Our ***brands, designs, patents,*** and ***other intellectual property***.
- The ***buildings*** and ***facilities,*** the ***furniture, fixtures*** and ***fittings,*** and the ***environmental working and surrounding areas*** and ***utilities*** we maintain to provide an acceptable working environment for people and technology.

2. Scope and Exceptions

This policy applies to:

- "M247" throughout its UK and International Sites (Trafford Park Logistics Centre & Turing House - Manchester; London and Bucharest – Romania)
- The protection and preservation of our ***business assets*** owned or retained for operational processing by M247 and its group operations as it operates from the UK and International Sites.
- All employees within the scope of this document, whether directly or indirectly employed or otherwise under the control of M247.
- All business assets of M247 within the scope of this document (as identified in section 4), wherever located, and for whatever purpose used and whether operated by an outside body on behalf of M247 or by M247 itself;
- All systems and information created, stored, or processed on networks, M247 endpoint devices provided by M247 within the scope of this document for business use when working from home or remote locations.

Exceptionally, relevant parts of this policy may be relaxed if complying with it would:

- lead to physical harm or injury; or
- cause significant damage to the company's reputation or ability to operate; or
- result in an illegal or improper act.

In such cases, employees must ensure that a Line manager of the company is made aware of the situation and involved in any decision making. The situation and circumstances should be recorded and reported to senior management and the security committee Sec.committee@m247.com as soon as possible.

The documentation is maintained electronically and consists principally of this policy together with any linked or referenced documents and records.

3. Principles of this Policy

Our security policy is aimed at the preservation of the ***confidentiality, integrity, availability, and legality*** of our business assets. Each of these attributes is explained in more detail below:

3.1. Confidentiality

Sensitive information (protectively marked, e.g. B-Internal, C-Confidential) shall only be made accessible to those who are ***authorised*** and with a ***genuine need to know***.

We shall respect the ***privacy*** and ***sensitivity*** of such information and shall handle it accordingly.

We shall ensure that customers' details, systems, and data are protected from unnecessary ***exposure*** or ***disclosure***.

We shall ***securely*** and ***promptly*** archive or dispose of information when no longer needed, or when we are required to do so by our customers.

3.2. Integrity

In the design and operation of our business processes and systems, we shall strive to safeguard the accuracy, completeness, and currency (timeliness) of information being processed.

3.3. Availability

We shall ensure that services, tools, and information are ***available*** for use by the right people (including our customers) at the right time with robust effective security controls. To this end we shall ensure changes to assets are made in a controlled manner, and promptly communicated to those with a need to know. The risks involved, and the impact of the change will be considered, and appropriate risk treatment measures will be put in place before any significant change is made.

To achieve planned availability, systems and processes need to be:

- *Adequately planned*
- *Correctly implemented*
- *Properly maintained*
- *Adequately documented*
- *Suitably decommissioned*

3.4. Legality

Our business operations and the services we deliver will be conducted in a legal manner, with due regard to our statutory duties and contractual obligations and will also comply with company rules and guidance. Failure to observe this policy may seriously compromise M247's business, its customers or its employees and may therefore result in disciplinary action and/or prosecution.

Any legal request should be sent to our legal@m247.com mailbox which will then be assessed and allocated to the correct team.

4. Context of the Organisation and Security Objectives

M247 context and information security objectives shall be S.M.A.R.T. and aligned with the organisation's mission, strategy /other (business) objectives. That is, to ensure:

The design, delivery, support and maintenance of bespoke infrastructure services including the provision of cloud, connectivity, hosting, telecommunications, and security services.

S.M.A.R.T

- Specific (simple, sensible, significant)
- Measurable (meaningful, motivating)
- Achievable (agreed, attainable)
- Relevant (reasonable, realistic, resourced, results based)
- Time Bound (time limited, based, cost limited, timely, time sensitive)

The applicable company Framework-Standard Manual shall define IS Objectives will be annually defined and updated. These will include specific and suitable KPI and Objectives.

5. Interested Parties

M247 define interested parties at the highest level as.

Party	Needs and Expectations
Employees	• Data protection • Working practices & procedures • Company rules • Contractual obligations
Shareholders/owners of the business	• Data protection • Contractual obligations • Performance & Monitoring
Government agencies/regulators	• Performance & Monitoring • Regulatory Requirements
Emergency services (e.g., fire brigade, police, ambulance, etc.)	• Performance & Monitoring • Regulatory Requirements
Customers	• Data protection • Site security • Service availability • Contractual obligations
Employee families	• Data protection • Performance & Monitoring
Media	• Performance & Monitoring
Suppliers and partners	• Data protection • Contractual obligations • Approval of suppliers • Performance & Monitoring

6. Security Policy

6.1 Security Policy Framework & Management Commitment

M247's business assets are primary resources upon which we and our customers depend for our present and future business prosperity. In exercising our responsibility to our stakeholders, we will take all reasonable and appropriate measures to ensure these assets are safeguarded from threats and vulnerabilities, and that business damage is prevented by minimizing the impact of security incidents.

We will take effective measures to ensure the security of business assets to maintain the levels of confidentiality, integrity, availability, and legality necessary to support the business.

We will work within a general operational, security management and compliance framework which includes the following codes of practice ***as a guide***:

- ***For information security*** - The standards and code of practice laid out in ISO/IEC 27001 & ISO 27000 series.
- ***For personnel security screening*** – Security screening of individuals employed in a security environment.
- ***For service delivery*** - ITIL and ISO 9001
- ***For fire security of data-centres*** - BS 6266 Code of Practice for Code of practice for fire protection for electronic equipment installations and ISO 45001 Standards

Security processes and controls will be reviewed (Quarterly) and improved to ensure their effectiveness. We will continue to review industry recognised best practices, and adopt these where they are appropriate (relevant, practicable and cost-effective) to our business.

This policy is supported by further detailed policies, processes and procedures which are documented in the collection of documents that support Security and operational policy and process within M247.

[PLEASE NOTE: such documentation may include highly sensitive information which must not be disclosed outside of M247 – even under Non-Disclosure Agreements (NDA). Doing so may constitute a security breach.]

Should you need any NDA information please contact compliance@m247.com or legal@m247.com

M247 will maintain budgets, plans and resources to sufficiently support this policy, appropriate to the prevailing or perceived levels of risk, and considering business trading conditions.

M247 will manage risk by identifying, controlling, and eliminating or minimizing risk to an acceptable level. Suitable risk assessment processes will be used to measure threats, vulnerabilities, and impact on business assets.

6.2 Organization of Business and Information Security

The following organization and responsibilities exist for the management of business and information security throughout M247:

6.2.1 Security Committee Forum

A senior management team whose representation includes those with responsibility for the key business assets governed by this policy. This includes:

Function	Role
CFO/Commercial Director	Responsible for supplier and third-party risk management
CTO	Responsible for Internal IT systems
Security Product Manager	Responsible for Security strategy and Products
Security Committee	Responsible for co-ordination of Information Security issues
SecOps Team Leader	Responsible for vulnerability and security operations
CPO/HR Director	Responsible for Human Resources
Risk and Compliance	Responsible for GRC at all levels

Other employees and advisors may be co-opted as required to address the business at hand.

The Security Committee Forum has the following roles and responsibilities, to:

- Provide strategy and high-level direction for security related matters.
- Agree overall responsibilities for information security.
- Review and approve information security policy.
- Ensure compliance with security policy throughout M247.
- Define M247's tolerance to Information Security risk; provide guidance on timescales, resources and budgets for security.
- Sponsor and track progress on major initiatives to enhance business and information security.
- Monitor significant changes in the exposure of information assets to major threats.
- Ensure the effectiveness of M247's security management is being reviewed and continually improved.

6.2.2 Security Committee

The Security Committee is responsible for:

- Development, promotion and support of M247's security policy.
- Maintaining this policy and providing practical advice and guidance on its implementation.
- Coordination of all major security related activities in M247.

- Providing general security awareness and training.
- Promoting services, standards, and procedures to support security objectives.
- Agreeing and supporting M247 security initiatives and projects.
- Ensuring security incidents and breaches are reviewed.
- Monitoring compliance with security policy.

6.2.3 Senior Management

Senior Managers are responsible for:

- Implementing Security Policy within their area of responsibility.
- Ensuring task-specific security training is provided for their colleagues.
- Ensuring that their colleagues remain security and risk aware.
- Ensuring that security incidents and breaches, weaknesses and vulnerabilities are being reported, and are addressed or escalated.

6.2.4 M247 Employees

All employees are responsible for:

- Ensuring they are familiar with, and comply with, security policy.
- Acting in a legal, ethical, and professional manner.
- Promptly reporting actual or suspected security incidents and breaches, weaknesses, and vulnerabilities to their line manager and/or senior management and the security Committee.

6.2.5 Business Asset “Owners”

Business asset "owners” are responsible for:

- Ensuring that adequate security is put in place for assets that existed before this policy was introduced.
- The day-to-day security of their business and information assets.
- Ensuring that all assets and security processes associated with each individual system is identified, defined, and documented.
- Ensuring that authorisation levels and procedures are clearly defined and documented.
- Ensuring that any delegated responsibility has been discharged correctly.

6.2.6 Project Managers

Project Managers implementing business systems are responsible for:

- Ensuring security of systems during development.
- Ensuring that security is designed and built-in to new systems for which they are responsible before deployment into a live environment.
- Providing security plans, processes, and documentation as a deliverable of the project before the system goes live.

6.2.7 People/Human Resources Team

The term “Employee” or” Colleague” includes permanent employees, part-time employees, and contractors.

The People Team are responsible for:

- Establishing appropriate employee policies with respect to business and information security.
- Ensuring security responsibilities are conveyed in contracts of employment, job descriptions and HR policy documentation.
- Security screening of employees and prospective employees, to assess their suitability for the roles they are/ will be performing.
- Ensuring that all employees receive adequate security training, and that records of such training is maintained; The CISO will be responsible for the Security Training.
- In association with line management and the CISO, to oversee any employee disciplinary processes relating to security.
- Ensuring that relevant areas of the business are informed of starters, leavers, and changes in employee status so that security controls (access rights, passwords, and permissions) can be adjusted in a timely manner.

6.3 Asset Management

An inventory will be maintained of key business assets. Business assets shall have an identified "Owner" and such owners shall have ownership, control and maintenance responsibilities associated and identified against the assets and their associated documents.

Policy and guidance exist in the employee handbook for the acceptable use of business assets, which employees are required to follow. Processes support policy which include but are not limited to the assignment of assets during or after the employee on-boarding process and the return of assets should employment be terminated.

We will protect important information assets by clearly marking documents and data according to their value, legal requirements, sensitivity, and criticality to M247. Procedures exist for correctly labelling and handling information according to its classification.

System and network configurations will be sufficiently documented. Such data will be protected against unauthorised access.

6.4 Human Resources Security

Background verification checks will be made on all candidates for employment, and contractors. Employment at M247 will only be offered if the candidate is suitably cleared and has the personal integrity to be given access to the information they will handle on a day-to-day basis without risk to the business.

We will maintain well defined job descriptions, contracts of employment and working practices for all employees, outlining security roles and responsibilities.

We will maintain a high-level of security awareness within the organization by ensuring that all employees receive regular job relevant security training. All employees must be aware that information security is an integral part of the day-to-day operation of company business; understand their individual responsibilities and be aware that business and information security is important to the company and to our customers.

Breach of security policy, including failure to report any violations of this policy may result in disciplinary action, including possible termination of employment, or even legal action if the violation is severe, or of a criminal nature.

6.5 Security in Operations Management

Operating procedures shall be documented, maintained, and made available to users who need them. Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organization's assets.

When engaging third parties in the delivery of our services, we will ensure that the security controls, service definitions and delivery levels included in the third-party service delivery agreement are implemented, operated, and being maintained by the third party.

Changes to the services we provide will be carefully managed to take account of the criticality of business systems and processes involved and re-assessment of risks.

The use of system resources will be monitored, tuned, and projections made of future capacity requirements to ensure that systems continue to provide the required levels of performance.

Acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the system(s) carried out during development and prior to acceptance.

We will deploy appropriate processes and tools for the prevention and detection of viruses and other malicious software on key information systems.

The use of mobile code will be carefully controlled to ensure that the authorised use operates according to a clearly defined security policy, and unauthorised mobile code is prevented.

We shall take regular back-up copies of information, software, and configuration details in accordance with the agreed backup policy. Backups will be tested regularly.

We will maintain procedures for the handling and storage of information to protect it from unauthorised disclosure or misuse. This will include procedures for the management of removable media. Media will be protected against unauthorised access, misuse or corruption during transportation and storage. Media will be disposed of securely and safely when no longer required.

We will monitor, manage, and control our internal networks, to protect them from threats, and to maintain security for the systems and applications using the network, and any information in transit.

Security features, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced.

We will carefully manage the exchange of information and software between M247 and external parties. Formal policies, procedures, and controls will be established where needed to provide adequate security.
Information involved in on-line transactions will be protected to prevent incomplete transmission, misrouting, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay.

We will protect the information being made available on publicly available systems from unauthorised modification.

Use of information processing facilities will be monitored and the records reviewed regularly. We will keep audit logs of user activities, exceptions, and information security events. System administrator and system operator activities will also be logged. These will be kept for an agreed period to assist in future investigations and access control monitoring. Logging facilities and log information will be protected against tampering and unauthorised access.

System faults will be logged, analysed, and appropriate action taken.
The timeclocks of all relevant information processing systems within M247 are to be synchronized with an agreed accurate time source.

6.6 Systems acquisition, development. & Maintenance

We will ensure that development, test, and operational facilities are separated to reduce the risks of damage, unauthorised access, or untested changes to the live environment.

The following are to be addressed during the design or selection of new information systems, or enhancements to existing information systems:

- Security requirements.
- Appropriate data validation checks to detect any corruption of information through processing errors or deliberate acts.
- Requirements for ensuring authenticity and protecting message integrity in applications shall be identified, and appropriate controls identified and implemented.
- Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.

Where appropriate to the level of risk, cryptographic controls will be used for the protection of sensitive information during transfer and storage. Cryptographic keys or certificates will be kept securely and prevented from unauthorised disclosure or use.

We will manage the introduction or modification to information systems through formal change control procedures. In particular:

- New software and updates will only be installed on operational systems under strict change control, having been through thorough testing. Any test data used shall be carefully selected, protected, and controlled.
- Source code will be restricted to only those with a direct need as a part of their job function, and with approval of the Director of Business Applications and Tools.
- Modifications to 3rd party software packages shall be discouraged, limited to necessary changes, and all changes shall be strictly controlled.
- Outsourced software development shall be supervised and monitored.

- When operating systems are changed, business critical applications will be reviewed and tested to ensure there is no adverse impact on operations or security.

6.7 Incident Management

M247 will continually **monitor key systems and infrastructure** to verify availability and operational effectiveness. M247 will maintain processes for responding to incidents affecting the business and the services provided to our customers.

M247 will regularly **gather information about technical vulnerabilities** of information systems being used. Exposure to such vulnerabilities will be assessed, and appropriate measures taken to address the associated risk to M247 and our customers.

Employees, contractors, and customers are required to **report any observed or suspected security weaknesses** in sites, systems, or services. Security events shall be reported through appropriate management channels as quickly as possible. Management shall ensure security incidents are responded to in a quick, effective, and orderly manner and that a suitable reporting system is used to track, resolve, and continually improve operational security at M247.

Incident statistics (types, volumes, and impact) will be gathered and periodically reviewed to ensure that incident management processes are effective and being continually improved.

Reporting Security Incidents

It is important that all security incidents are reported immediately;

a. All users must report known or suspected password compromises.
b. All instances of suspected disclosure of sensitive information must additionally be reported. This is especially time-critical for sensitive data and information systems that store sensitive data.
c. Additionally, all users must promptly report to the M247 Security Committee any loss of or severe damage to their hardware or software. For example, if a portable computer is stolen, the theft must be reported.
d. Users must also report all suspected compromises to M247 data/information systems.
e. If information security vulnerability is discovered or known to exist in any network or system, this too must be reported.
f. Any other instance of security, data or information breach

Client Notification - Clients whose data has been impacted by a security incident will be notified per the terms of their agreement and M247 reporting processes. All client notifications concerning security incidents are to be approved by M247 Senior Leadership after notification from the M247 Security Committee sec.committee@m247.com.

Incident Management - All users must report suspected or known security violations to M247 Security Committee and if required, Hosting/Infrastructure teams.

Incident Evaluation - The evaluation of information security incidents might indicate the need for enhanced or additional controls to limit the frequency, damage, and cost of future occurrences.

Evidence Collection - Where a follow-up action against a person or organisation after an information security incident involves legal action (either civil or criminal), evidence should be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s). Requirements for evidence collection will be supplied by M247 Security Committee through the Legal Team.

Any **forensics work** should only be performed on copies of the evidential material. The integrity of all evidential material should be protected. Copying of evidential material should be supervised by trustworthy personnel and information on when and where the copying process was executed, who performed the copying activities and which tools and programs have been utilised should be logged.

Where a **follow-up action** against a person or organization after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

How to Log a Security incident – MetaCompliance - In order to Log a Security Incident or event please go to https://cloud.metacompliance.com/Account/Login

- Log in to your account with your M247 email and MetaCompliance password;
- Once Logged in select Report Incident.
- Select Add Incident;

Examples of items to report – Data Breach sent an email to the wrong person, tailgating onsite, unknown person onsite or in-office areas without escort, suspected phishing emails, data left in public area, virus or malware issues.

- Complete the incident log, you will need to detail,
- Once Completed, please select submit, you will also receive an email to confirm this has been logged and will be dealt with by a senior employee.

If you have any questions regarding this process please contact the security committee directly on sec.committee@m247.com

6.8 Business Continuity Management

A business continuity management process is in place to reduce the disruption caused by disasters and security failures to an acceptable level through a combination of preventive and recovery controls.

Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security.

Plans shall be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.

Business continuity plans shall be tested and updated regularly to ensure that they are up to date and effective.

6.9 Compliance

M247 will comply with all legislative and regulatory requirements relevant to information assets in all jurisdictions in which it operates. In particular, the following areas of law are specifically applicable to the security and operations of our business:

- UK Data Protection Act (2018)
- EU GDPR (2016)
- Computer Misuse Act 1990
- Telecommunication Regulations 1998
- Regulation of Investigatory Powers Act 2000 (RIP Act)
- The Privacy and Electronic Communications Regulations 2003
- Copyright, Designs and Patents Act 1988 [Piracy of software, music and any other copyrighted work is strictly prohibited.]
- Health and Safety at Work Act 1974
- Companies Act 1985
- Human Rights Act 1998
- Digital Economy Act 2017
- Control of Major Accident Hazards Regulations 2015
- NIS Guidelines 2018
- Telecoms Security Act 2021

Important records shall be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements.

Information systems shall be regularly checked for compliance with security implementation standards.

It is the responsibility of the Security Committee to assess new information systems or upgrades and to test any new system or upgrade for its suitability of implementation across the organisation. Any new system is to be installed and tested in an isolated fashion before implementation to a production environment.

Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to minimize the risk of disruptions to business processes.

Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.

7. Policy Review and Evaluation

This policy is the responsibility of the Business itself and the R&C Lead, who will maintain and review it according to the following guidelines:

The policy will be reviewed in response to:

- Significant changes to business organization or structure.
- New or significantly revised business assets.
- Changes to threats & vulnerabilities.
- External factors (environmental, social, political).

The policy will be reviewed annually for:

- Its effectiveness, demonstrated by the nature, number and impact of recorded security incidents.
- Cost and impact of controls on business effectiveness.
- Effects of changes to technology.

Changes to this policy must be approved by the Security Executive Forum and communicated to all employees affected.

8. Internal Audits

An internal Audit programme shall be implemented and executed according to the Internal Audit Programme Schedule. Findings from such audits shall be reported to appropriate management and such outputs shall be used to facilitate improvements where required.

Internal Audits shall be conducted by competent personnel.

Internal Audit outputs and identified improvements shall be reviewed during management review for effectiveness and to ensure identified improvements have been addressed.

Records of Internal Audits, the schedule, checklists, evidence, and records shall be securely stored.

Such records shall be used within Management Review meetings to review improvements made.

9. Continual Improvement

Based on outputs of pro-active actions such as audits and meetings or retro-active actions such as security events, security incidents or other outputs identified within this policy and associated documents, M247 shall ensure a continual improvement methodology is used and awareness of such a methodology shall be intrinsic to all security related training activities.

Essential actions to such a methodology are.

1. To determine and resolve the immediate challenge *(reporting to regulatory bodies where required)*
2. To investigate and document the root cause
3. To take action to prevent future occurrence *(or have the option to decide not to where appropriate)*
4. To maintain related records
5. To review such records and challenges during Management Reviews

10. CEO/CFO Statement

M247 is committed to implementing policy and controls that fulfil our requirements for information security, along with continual improvement of our information security management system.

Signed: D Edwards Date: 21.09.2022 Review Date: 21.09.2022

D Edwards - CEO

_____

11. Review

This policy will be reviewed at least every 12 months.

12. Changelog

Version	Date	Comments	Name	Title	Function
0.1	17/07/2017	First Draft Assembly/Transition (CIO/Group Information Security Manager)	Gary Thomlinson, Gary Myers	Head of Risk and Compliance, Group Information Security Manager	Author
0.2	21/07/2017	Addition of continual improvement, internal audit, and objectives. (Group Information Security Manager)	Gary Thomlinson, Gary Myers	Head of Risk and Compliance, Group Information Security Manager	Author
0.3	07/08/2017	Continued evolvement of pre-release document	Gary Thomlinson, Gary Myers	Head of Risk and Compliance, Group Information Security Manager	Author
1.1	08/08/2017	Release authorised. V1.1 set as this document supersedes the original V1.0 (that was version dated rather than incrementally versioned) document for TP.	David Warburton-Broadhurst	CIO	Approver
1.2	14/08/2017	Updated Legal Entities	Gary Thomlinson	Head of Risk and Compliance	Author
1.3	06/11/2018	Reviewed and rebranded	Gary Myers	Group Information Security Manager	Author
1.4	08/11/2018	Reviewed by CEO, minor changes made for clarity	Jenny Davies	CEO	Author
1.5	17/09/2019	Review with AT to update and check requirements	Gary Myers and Andrew Turner	Group Information Security Manager	Author
1.6	16/09/2020	Review with AT to update and check requirements	Gary Myers, Andrew Turner	CISO	Author
V1.7	04.08.2021	Updated Owner, Reviewed and changed Exec Owner	AJT	R&C	R&C

V2.0	21.09.2022	Updated with Sec team and added in TSA requirements	AJT	R&C	R&C