Security Policy

1. Introduction

BM Group here under referred to as the 'Company' understands the importance of data security and makes every effort to ensure that customer data held on systems and within the data centres are fully protected.

The Company recognizes that the confidentiality, integrity and availability of information and data created, maintained and hosted by Company the Company and its customer's is vital to the success of the business.

The Company's management view these as primary responsibilities and fundamental to best business practice and as such has adopted the Information Security Management System Standard BS ISO/IEC 27001:2013 and PCI DSS as its means to manage and meet the following objectives:

1.1. Comply with all applicable laws, regulations and contractual obligations including the Data Protection Act (GDPR).
1.2. Implement continual improvement initiatives, including risk assessment and treatment strategies, while making the best use of its management resources to meet and improve information security system's requirements.
1.3. Communicate its Information Security objectives and its performance in achieving these objectives, throughout the Company and to interested parties.
1.4. Adhere to the Information Security Management System (ISMS) comprising of a security manual and procedures that provides direction and guidance on information security matters relating to employees, customers, suppliers and interested parties who come into contact with the Company's work.
1.5. Work closely with their customers, business partners and suppliers in seeking to establish Information Security Standards.
1.6. Adopt a forward-looking view on future business decisions, including the continual review of risk evaluation criteria, which may have an impact on Information Security.
1.7. Train all members of staff in their needs and responsibilities for Information Security Management.
1.8. Constantly strive to meet, its customers and staff expectations.
1.9. Information Security shall be considered in job descriptions and when setting staff objectives where applicable.
1.10. Appropriate Information Security training and awareness shall be provided to all staff to ensure principals and practices are embedded in the company culture.

2. Purpose

The purpose of this document is to provide information about the procedures Company maintains to ensure the security of its customers' data, software and systems.
This document will cover the following areas:

1. Customer Authentication
2. Physical Security
3. Access Control
4. Network Security
5. Software Security
6. Media Handling
7. Auditing and Monitoring
8. Contingency Planning
9. Recruitment and Training

This policy applies to all Company employees or any other individual or supplier working for Company. Company management team are responsible for ensuring full compliance with this policy.

Unless written permission is obtained by the ISMS chairperson, no part of this policy and other relevant policies can be ignored or bypassed. It is the responsibility of all staff members to report any such incidents in a timely fashion. It is the responsibility of the ISMS to review such incidents and identify the correct course of action.

The CTO was appointed by the management to provide an annual executive summary of the ISMS.

3. Data Protection

Company is committed to complying with data protection legislation as documented in AD-POL-2018-003 - General Data Protection Policy and good practice including:

- processing personal information only where this is strictly necessary for legitimate organisational purposes;
- collecting only the minimum personal information required for these purposes and not processing excessive personal information;
- providing clear information to individuals about how their personal information will be used and by whom;
- only processing relevant and adequate personal information;
- processing personal information fairly and lawfully;
- maintaining an inventory of the categories of personal information processed by the Company;
- keeping personal information accurate and, where necessary, up to date;
- retaining personal information only for as long as is necessary for legal or regulatory reasons or, for legitimate organisational purposes;
- respecting individuals' rights in relation to their personal information, including their right of subject access;
- keeping all personal information secure;
- only transferring personal information outside the EU in circumstances where it can be adequately protected;
- the application of the various exemptions allowable by data protection legislation.

4. Customer Authentication

Any support requests sent to the Company from Customers, for information about their service or to request assistance must be validated to ensure they are who they say they are. This will reduce the risk of loss of confidentiality and data breaches.

In the event that an unauthorized individual contacts the Company:

- The procedures and policies outlining authorization requests, including a blank authorization form if onetime only, are provided to the client who is advised to have these filled by an authorised contact;
- No requests are entertained from the unauthorized client;
- An e-mail is sent to the Authorised official and/or contract signatory with the name and request of the individual requesting access.

5. Physical Security

The Company's data centre facilities are diversely located in Handaq and Smart City Malta and connected by secure, resilient high speed back-up links. Both of our data centres have the following physical security features in place to protect both equipment and customer data.

All racks within the data centres are equipped with fully lockable doors which only authorised engineers have access to. Proximity door locks are fitted on all internal and external doors and extensive CCTV monitoring systems are installed on all internal and external walls.

CCTV monitoring systems include motion detection features that trigger CCTV recording in the event of any movement both inside and outside of the data centres (within the cameras' range).

Company operates Uninterruptible Power Supply (UPS) systems and diesel generators on all of it sites to ensure that services remain available in the event of a power failure.

Full access control systems are in place that only allows authorized employees to secure areas; no other employees, customers or third parties are authorised to access these areas unless accompanied by an authorised engineer.

Any visitor access is strictly as per AD-PRC-2011-002 - Authorisation Clearance. All visitors are required to provide one week's prior written notice of their visit and produce photo ID upon arrival at the data centre. The visitor's log sheets are kept indefinitely.

All Company staff are required to carry their site access and identification card with them at all times and access is restricted to authorised areas only. The Company's management team reserves the right to refuse access to anyone without a site access card.

6. Access Control

Access to Company's internal systems, data floors, hosting platform and customer infrastructure is permitted for authorised personnel only. All persons must be positively identified by providing a secure User ID and password before being given access to system resources.

Access rights (privileges) to system access are given only to the users who need to access the system. The access rights given to each user are recorded in the Access Declaration Form, document number AD-FOR-2011-019.

When remote access is required, a VPN connection must be used. Attempts to circumvent using the VPN connection for remote access are considered as a serious breach of security.
Users are only granted a logon by the explicit approval of the C.T.O. and corresponding form AD-FOR-2011-019 must be filled accordingly. Usernames and passwords for VPN users must follow the password policy.

The VPN must, at a minimum have:

- two factors of authentication:
- Encryption;
- Be unique to each user.

Only Company's Core Engineers have full access to the hosted platforms, each engineer having their own individual login for optimum security. Authorised support staff have limited access to hosted services in order to provide technical support to customers.

7. General Security and Passwords

- Any computer terminal with access to Company data must follow Company's security policies. The user is responsible for the security of any computer terminal being used. Each unattended terminal needs to be locked, in order to prevent unauthorised users accessing the system.

- Users need to select secure passwords. Passwords should not be dictionary words and should not have personal identifiable and guessable information. Passwords must not be stored or transmitted in plain text. Passwords should not be lent. Company reserves the right to enforce the password selection process and to audit such at intervals.

- Company has a clear desk and clear screen policy. It is expected that all confidential information in hardcopy or electronic form is secure, particularly at the end of the day and when expected to be away for an extended period of time.

8. Acceptable Use

8.1 Internet files and software

Employees must not download or accept any software that is not required for business purposes. Employees must screen all files downloaded from the Internet with virus detection software.
Employees must not make illegal copies of copyrighted software. All software used on employees' computers within the firm must be a licensed copy and must adhere to the software owner's copyright conditions.

8.2 Monitoring of Internet use

the Company reserves the right to monitor and log all connections between their networks and the Internet. These logs include the user's name and those of the sites accessed. Such activity will be kept as per the retention policy.

8.3 Blocking of internet sites

The Company reserves the right to block access to any Internet site or resource deemed inappropriate.

8.4 Access rights

Users who do not have administrative accesss must NOT try to circumvent such enforcements. If users are found to have breached such security, disciplinary action might be enforced. This includes:

- Making changes to circumvent security software or other restrictions in place;
- Using systems that are not authorised by the Company to store and/or process data;
- The use of portable applications that are against policies;
- Making systems unavailable for one or more users through the use of unauthorised network devices;
- Attempting to impersonate other users.

9. Network Security

The network design is intended to deliver high performance and reliability to meet the needs of the operations whilst providing a high degree of access controls and range of privilege restrictions. The configuration of network impacts directly on its performance and affects its stability and information security. The network design takes into consideration that:

- Poor network stability can threaten operations;
- Inadequate control over access to network can jeopardize the confidentiality and integrity of data;
- Slow or inadequate system response times impede the processing.

9.1 Managing the network

The network is managed by the Core Team. Changes must be analysed for any potential security risk introduction.

9.1.1. Accessing network remotely

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. The needs for remote access are to be clearly defined before it is granted. Users which require remote access will often be connecting through public unsecure networks. This increases the threat of unauthorized access - therefore all individuals with remote access need to be advised of the risks and follow the procedure which is put in place governing how they connect to the intranet.

9.1.2. Defending network information from malicious attack

All system hardware, operating and application software, the networks and communication systems are safeguarded at all times from physical access or network intrusion. All physical hardware is kept within designated rooms and/or cabinets which can only be accessed by the technical staff. The technical staff is also responsible for ensuring that all network access points are secured. Unused ports are to be kept in disabled status on the network device. Non IP authorized systems are denied access to critical systems.

Network cabling is also segregated from Power cabling to ensure no interference is experienced. Special cable trays exist within the designated areas for cable runs to be passed neatly and safely to make sure they are not affected.

Access to designated areas is defined by the user's job requirements and controlled by their card access.

10. Software Security

Company's Core Engineers are responsible for all software security updates on Company's infrastructure.

Company operates a strict software security policy throughout the organisation to provide increased security across the network; this is governed by an IT Code of Conduct.

All software loaded onto Company's IT systems must be legally purchased and licensed and access to install programmes is restricted to members of the Core team only. Any application launched on Company's infrastructure must have its suitability verified by Company's Core Department and approved by the CTO prior to rollout

Furthermore, Company employees must ensure that systems are conforming to security policies set up by the company. The employee must NOT in any way tamper or impede with these operations:

- Anti-Malware software is installed, up to date and allowed to perform regular scans;
- The software firewall is enabled and maintained properly;
- Secure methods are used to transfer files;
- Authentication is set up on all systems;
- User is logged out following inactivity periods;
- Understand the features installed are to assist with security and not hinder the user;
- Use a high security level on your Internet browser;
- Never share any details on security.

11. Media Handling

11.1 Media handling as classified

Information classification is extremely important as the information handling process is built upon it. The list below identifies the basic handling guidelines for the data as classified. It is noted that identified data assets may be subject to specified handling as listed on Company's ISMS management system.

11.2 Public and unclassified media

Markings: None required
Physical and Logical Controls: None required
Reproduction: Unlimited or as per Copyright
Distribution: No restrictions
Disposal: Trash

11.3 Confidential

11.3.1 Internal use

Markings: Documents should be marked for *Internal Use Only*
Physical and Logical Controls: The author should make sure proper markings are in place. Users are required to ensure information is stored and controlled.
Reproduction: Limited copies may be made only if necessity arises.
Distribution: Internal unrestricted; External sealed envelope; Electronic use encryption for external transmission; Fax ensure details are correct.
Disposal: Printed media shredded; Electronic media sent to 2nd Level support for correct archiving or media disposal as per media handling policy.

11.3.2 Other

Markings: Documents must be marked as Confidential
Physical and Logical Controls: Author is responsible for ensuring information is not available for distribution and is clearly marked. Recipients must not share the information.
Reproduction: Limited copies may be mode under the approval of the original distributor.
Distribution: Internal - sealed envelope; External - sealed envelope and sent by registered mail or hand delivered; Electronic - encrypted; Fax - requires test page with phone confirmation prior to sending actual documentation.
Disposal: Printed media - shredded; Electronic media - sent to 2nd Level support for correct archiving or media disposal as per media handling policy.

11.4 Disposal of media

The disposal of client's media is the sole responsibility of the client and Company the Company is not responsible for the safe disposal and/or destruction of said media.

Where the media belongs to the Company, the media is archived permanently in secure storage with limited access. Where the need arises for the backup media to be disposed entirely, it must be destroyed through appropriate means and where required, a certificate for the destruction of media is issued accordingly from the responsible parties for the destruction.

Paper media must be shredded. It is often best to shred multiple sheets at the same time to help ensure that the contents cannot be reassembled.

12 Auditing and Monitoring

Having visibility of the activity ongoing on the network infrastructure is crucial to maintain the expected level of service availability, performance and security. All Company Core Networking equipment (switches and routers) must keep an activity log on an external syslog server. Modify access to the syslog server is restricted to the core team.

Every day an automated script checks all the logs on each server and analyses the content. It then emails a report to the core team with any warnings found. If no warnings are found, a report is still sent to advise the green status of the equipment.

All issues are logged by Service Requests and major faults or problems relating to the network are escalated to the Core team and/or CTO accordingly.

13 Contingency planning

In line with our ISO 27001 certification, Company operates its own disaster recovery procedures. In the event of any security issue being identified, an escalation process is in place whereby engineers are alerted by Service Request. Upon completion of the remedial work and resolution of the fault, the Service Request is closed.

Company has a continued, ongoing commitment to data security and availability. In addition, Company reserves the right to take all contractual allowable measures in respect of a customer's service if it is believed that the use of the service constitutes a security threat to Company or any other users/customer on Company's infrastructure.

14 Recruitment and Training

All candidates employed by Company are subject to screening. As part of this process, all references are followed up for new employees and security training is included within both the induction training programme and also ongoing.

Company implements an internal IT Code of Conduct that all employees must adhere to so as to ensure security and integrity of software, systems, hardware and data, in line with the requirements of ISO 27001 and PCI DSS. All employees with operational responsibilities are subject to Baseline Personnel Security Standard checks.