FOSROC

constructive solutions

IT Security Compliance

JMHFosroc_ITPOL-002

Author	Michael Alford
Author's Position	IT Helpdesk Manager – Asia
Date	6th October 2011
Version Number	2.0
Next Review	June 2021

Amendment History

Rev	Amendment Details	Prepared By	Reviewed By	Issue Date
1.0	Initial release	Tony Colbourne		18/06/09
1.1	Updated	Tony Colbourne		22/06/09
1.2	5.5 Data Security Access 5.6 JMHGroup Software Licensing	Tony Colbourne		29/06/09
1.3	General review of policy. Included author and sign off table. Spelling and grammar corrections. Update of link on page 8	Michael Alford	Aneel Khuram David Doherty	06/10/11
1.4	Yearly review of document	Michael Alford	Aneel Khuram David Doherty	27/01/2012
1.5	IT Asset Disposal procedure link added to section 5.4	Michael Alford	Aneel Khuram David Doherty	01/03/2012
1.6	Updated sign-off section Section 5.2 paragraph 2 updated with http://Link rather than data stored to file servers Section 5.4 Asset disposal link update to point to location on http://Link Section 5.5 link to IT Password Policy updated	Michael Alford		08/02/2015
1.7	Added Introduction section from GDPR Toolkit Updated Policy Statement, Purpose and Scope sections from the GDPR Toolkit Removed Definition and Risks Section	Tommy Ashton	Naser Sultan	08/06/2018

	Added Heading 6. Procedures and Guidelines Added 6.4 Security Classification, 6.5 Access to Information, 6.6 Secure Disposal of Information, 6.7 Re-Use of Equipment, Information on Desks, Screens and Printers, 6.10 Data Encryption, 6.11 Remote Access, 6.12 Firewall and Malware Added 7. Security Breach Management Added 8. Responsibilities Removed from old policy 4. Definition 5. Risks 6. Policy Compliance 7. Review and Revision, 8. Key Messages 9. Support, 10 Enforcement and 11 Change			
1.8	1.0 Updated Hyperlinks to other IT policies General clean-up of spelling and Grammar 6.1 Provided definitions of Confidential and restricted data 6.1.1 Remote Policy - Added hyperlink to the network policy Add Neil to the Sign off section Changed Page Footer to new format	Tommy Ashton	Neil Cowling	18/09/2018
1.9	Updated to reflect Group IT Organisational Realignment changes	Neil Cowling		15/07/2019
2.0	Annual review and amendment to sections 6.7 and 6.8	Neil Cowling		20/06/2021

Sign Off

Name	Signature	Date
Ian Watt CEO		08/06/18
Naser Sultan Vice President – Corporate Services		08/06/18
Neil Cowling		08/06/18

Group IT Manager		

CONTENTS:

1 INTRODUCTION 5

2 POLICY STATEMENT 5

3 PURPOSE 6

4 SCOPE 6

5 OBJECTIVES 6

6 PROCEDURES & GUIDELINES 7

6.1 SECURE AREAS 7
6.2 EQUIPMENT SECURITY 8
6.3 SECURITY OF EQUIPMENT OFF PREMISES 9
6.4 ACCESS TO INFORMATION 10
6.5 SECURE DISPOSAL OF INFORMATION 10
6.6 RE-USE OF EQUIPMENT 11
6.7 DATA SECURITY 11
6.8 DATA ENCRYPTION 11
6.9 INFORMATION ON DESKS, SCREENS, AND PRINTERS 12
6.10 JMH GROUP SOFTWARE LICENSES 12
6.11 REMOTE ACCESS 13
6.12 FIREWALLS AND MALWARE 13

7 SECURITY BREACH MANAGEMENT 14

7.1 INTRODUCTION 14
7.2 BREACH MANAGEMENT APPROACH 14

8 RESPONSIBILITIES 15

1 Introduction

The JMH Group *(hereinafter referred to as the **"Company"**)* has an extensive and robust Information Security Program that consists of policies, procedures, controls, and measures. This Information Security Policy is the foundation of this program and ties together all other policies as they relate to information security and data protection.

The Company Information Security Policy covers all aspects of how we identify, secure, manage, use, and dispose of information and physical assets as well as acceptable use protocols, remote access, passwords, and encryptions. To ensure that the importance of each information security area is not missed or vague, we use separate policies and procedures for each information security area and where applicable, reference these external policies in this document.

All information security policies and procedures should be read and referred to in conjunction with each other, as their meaning, controls, and measures often overlap. The policies and documents that form part of the Company information security programme are:

- Email and Internet usage Policy
- Network Connection Policy
- ERP Systems Usage Policy
- IT Password Policy
- Intranet Policy
- IT Purchase Policy
- Computer Procurement Policy
- IT Asset Disposal Procedure
- Mobile Device Policy
- Data Retention & Erasure Policy
- Data Protection Policy & Procedure

2 Policy Statement

Information and physical security are the protection of the information and data that the Company creates, handles, and processes in terms of its confidentiality, integrity, and availability from an ever-growing number and wider variety of both internal and external threats. Information security is extremely important as an enabling mechanism for information sharing between other parties.

The Company is committed to preserving information security of all physical, electronic, and intangible information assets across the business, including, but not limited to all operations and activities.

The Company aims to provide information and physical security to:

- Protect customer, 3rd party, and client data
- Preserve the integrity of the Company and its reputation
- Comply with legal, statutory, regulatory, and contractual requirements
- Ensure business continuity and minimum disruption
- Minimise and mitigate against business risk

3 Purpose

The purpose of this document is to provide the Company's statement of intent on how it provides information security and to reassure all parties involved with the Company that their information is always protected and secure from risk.

The information the Company manages will be appropriately secured to protect against the consequences of breaches of confidentiality, failures of integrity, or interruptions to the availability of that information.

4 Scope

This policy applies to all staff within the Company *(meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns, and agents engaged with the Company)*. Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

5 Objectives

The Company has adopted the below principles and objectives to outline and underpin this policy and any associated information security procedures:

- Information will be protected in line with Company data protection and security policies and associated regulations and legislation, including but not limited to EU General Data Protection Regulations, human rights, and the Freedom of Information Act.

- All information assets will be listed in the IT Service Desk Asset database by the IT Service Desk and will be assigned a nominated owner who will be responsible for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect it.
- All information will be classified according to an appropriate level of security and will only be made available to those who have a legitimate need for access and who are authorised to do so.
- It is the responsibility of all individuals who have been granted access to any personal or confidential information to handle it appropriately in accordance with its classification and the data protection principles.
- Information will be protected against unauthorised access and encryption methods will be used.
- Compliance with this policy and associated policies will be enforced and failure to follow either can result in disciplinary action.

The VP - Corporate Services has the overall responsibility for the governance and maintenance of this document and its associated procedures and will review this policy at least annually to ensure it is fit for purpose and compliant with all legal, statutory, and regulatory requirements and rules. It is the sole responsibility of the VP - Corporate Services to ensure that these reviews take place and to ensure that the policy set is and remains internally consistent.

6 Procedures & Guidelines

6.1 Secure Areas

CONFIDENTIAL and RESTRICTED information must be stored securely. A risk assessment should identify the appropriate level of protection to be implemented to secure the information being stored.

- Confidential Information – The term “confidential information” applies broadly to information for which unauthorised access or disclosure could result in an adverse effect. To address this risk, some degree of protection or access restriction may be warranted.
- Restricted Information – “Restricted Information” is a term for the most sensitive confidential information. Restricted information or data is any confidential or personal information that is protected by law or policy and that requires the highest level of access control and security protection, whether in storage or in transit.

Physical security must begin with the building itself and an assessment of perimeter vulnerability must be conducted. The building must have **appropriate** control mechanisms in place for the type of information and equipment that is stored there. These could include, but are not limited to, the following.

- Alarms fitted and activated outside working hours
- Window and door locks
- Window alarm sensors on lower floor levels
- Access control mechanisms fitted to all accessible doors (where codes are utilised, they should be regularly changed and known only to those people authorised to access the area/building)
- CCTV cameras
- Staffed reception area
- Protection against damage - e.g. fire, flood, vandalism

As an example, access to secure areas such as the data centre and IT equipment rooms must be adequately controlled and physical access to buildings should be restricted to authorised persons. Staff working in secure areas should challenge anyone not wearing an identification tag. Each department must ensure that doors and windows are properly secured.

Identification and access passes (e.g. badges, keys, entry codes etc.) must only be held by employees authorised to access those areas and should not be loaned /provided to anyone else.

Visitors to secure areas are required to sign in and out with arrival and departure times and are required to wear an identification badge. A Company IT employee must always monitor all visitors accessing secure IT areas.

Keys to all secure areas housing IT equipment and lockable IT cabinets are held centrally. Keys are not stored near these secure areas or lockable cabinets.

In all cases where security processes are in place, instructions must be issued to address the event of a security breach. Where breaches do occur, or a member of staff leaves outside normal termination circumstances, all identification and access passes (e.g. badges, keys etc.) should be recovered from the staff member and any door/access codes should be changed immediately. Please also refer to the JMHGroup IT Staff Leaving Checklist.

6.2 Equipment Security

All general computer equipment must be located in suitable physical locations that:

- Limit the risks from environmental hazards – e.g. heat, fire, smoke, water, dust, and vibration.
- Limit the risk of theft – e.g. if necessary, office doors and windows should be secured at the end of the working day.
- Allow workstations handling sensitive data should be positioned to eliminate the risk of the data being seen by unauthorised people.

Desktop PCs should not have sensitive data stored on the local hard drive. Data should be stored on http://Link where appropriate. This ensures that information lost, stolen, or damaged via unauthorised access can be restored with its integrity maintained. Laptops and desktop Computers will be BIOS protected to prevent access to Company data following theft. For sites that don't have access to http://Link, all sensitive data should be stored on the local file server with the correct share and security permissions applied. User working files stored in workstation standard folders (documents, desktop, pictures) will be backed up to the encrypted Microsoft OneDrive cloud-based solution to enable quick recovery in the event of an attack or disk failure.

All servers located outside of the data centre must be sited in a physically secure environment. Business critical systems should be protected by an Un-interrupted Power Supply (UPS) to reduce the operating system and data corruption risk from power failures. The equipment must not be moved or modified by anyone without authorisation from the Group IT Manager or the VP - Corporate Services.

All items of IT equipment must be recorded in the IT Service Desk Asset Database. Procedures should be in place to ensure inventories are updated as soon as assets are received or disposed of.

All equipment must be security marked and have a unique asset number allocated to it. This asset number should be recorded in the Departmental and the IT Service Desk asset database.

6.3 Security of Equipment Off Premises

All IT staff and 3rd party suppliers must ensure that all JMH Group IT equipment is maintained in accordance with the manufacturer's instructions and with any documented internal procedures to ensure it remains in working order.

- Identify recommended service intervals and specifications
- Enable a call-out process in event of failure
- Ensure only authorised technicians complete any work on the equipment
- Record details of all remedial work carried out
- Identify any insurance requirements

- Record details of faults incurred, and actions required

A service history record of equipment should be maintained so that as equipment ages, decisions can be made regarding the appropriate time for disposal and/or replacement.

Equipment maintenance must be in accordance with the manufacturer's instructions. This must be documented and available for support staff to use when arranging repairs.

6.4 Access to Information

Staff at the Company will only be granted access to the information they need to fulfil their role within the organisation. Staff who have been granted access must not pass on information to others unless they have also been granted access through appropriate authorisation. Even where access has been granted, additional authorisations may be needed to view, read, manipulate, or edit this information. It is the employee's responsibility to ensure that they have the necessary approvals.

Requests to grant, change or remove access to Company information is via the Automated System Access request forms which can be accessed via the Fosroc Link - Systems Access Portal tile.

This information is then tracked through raising a request with the IT Service Desk.

6.5 Secure Disposal of Information

Care needs to be taken to ensure that information assets are disposed of safety and securely and confidential paper waste is disposed of in accordance with relevant procedures on secure waste disposal. Where an external shredding service provider is employed, secure paper disposal bins are in each office and used in all instances of confidential paper disposal.

Electronic information must be securely erased or otherwise rendered inaccessible prior to leaving the possession of the Company unless the disposal is undertaken under contract by an approved disposal contractor.

In cases where a storage system (for example a computer disc) is required to be returned to a supplier, it should first be securely erased unless contractual arrangements are in place with the supplier which guarantee the secure handling of the returned equipment.

Software media must be destroyed to avoid the possibility of inappropriate usage that could breach the terms and conditions of the licenses held.

Details on the proper disposal of IT assets can be found in the IT Asset Disposal Procedure:

IT Asset Disposal Procedure

6.6 Re-Use of Equipment

PCs or laptops that are to be reused will be re-imaged via SCCM to the default JMH Group build before being deployed to a new user. Smartphones or Tablets that are to be reused will be reset to factory defaults via AirWatch or factory reset before being deploying to a new user.

6.7 Data Security

All Company data stored on our Production servers located in the Singapore Data Center will be backed up daily, first to disk via StoreOnce and then to tape, which is then stored in a secure offsite facility (Please refer to Fosroc's backup Procedure). Critical Fosroc data is also replicated to our Dubai based Disaster Recovery Data Center as identified in the Group IT Disaster Recovery Plan.

Company users must store all business documentation on their relevant OpCo or Functional area within SharePoint (LINK). User working files stored in workstation standard folders (documents, desktop, pictures) will be automatically backed up to the encrypted Microsoft OneDrive cloud-based solution to enable quick recovery in the event of an attack or disk failure.

Access to workstation USB ports for storage devices has been restricted. This prevents the introduction of malware via removable media such as thumb drives and external hard drives.

A small number of users are currently exempt from the USB restrictions as mentioned above, as approved by their VPs. These users have been provided with company encrypted external USB drives to back up their data until the One Drive project is completed. No other external USB storage devices apart from company issued ones should be connected to workstations.

Any employee seeking to remove sensitive data off site should obtain permission from a General Manager or VP.

6.8 Data Encryption

Encryption methods are used to protect confidential and personal information within the Company and when transmitted across data networks. Encryption methods are also employed when accessing Company network services, which requires authentication of valid credentials (usernames and passwords). All JMH Group network traffic across the Wide Area Network (WAN) is protected by industry standard encryption.

Where confidential data is stored on or accessed from Company owned mobile devices (for example, laptops, tablets, smartphones, approved external hard drives, the devices will be encrypted and configured by Group IT to protect the data contents. Company data, whether confidential or not, must never be stored on personal devices. No confidential data should be

stored in public, cloud-based storage facilities unless approved by a respective VP and Group IT Manager. If approved, then the cloud account must be created using a Fosroc email address / ID and the details stored with the IT Service Desk. Once approved, the data must be encrypted prior to storing in the public or cloud storage to ensure that it is not possible for the service provider to decrypt the data.–Where data is subject to an agreement with an external organisation, the data should be handled (stored, transmitted, or processed) in accordance with the organisation's specified encryption requirements.

Where there is a requirement to transfer personal information outside the Company, it is always kept in an encrypted format.

6.9 *Information on Desks, Screens, and Printers*

Members of staff who handle confidential paper documents should take the appropriate measures to protect against unauthorised disclosure, particularly when they are away from their desks. Confidential documents should be locked away overnight, on weekends, and at other unattended times.

Care should also be taken when printing confidential documents to prevent unauthorised disclosure. Confidential documents should be retrieved from printers as soon as they are printed and not left lying uncollected.

Computer screens on which confidential or sensitive information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorised persons. All computers must be locked while unattended.

To ensure access to Company data is restricted, all users are required to lock their workstation if unattended for any period of time. There is also a Company policy automatically applied to lock an unattended workstation after a short period of inactivity. Domain passwords will be updated monthly and subject to rigorous requirements regarding sophistication such as minimum requirement of characters and a mixture of upper- and lower-case letters and numbers. For more information on password requirements please see the JMH Group password policy IT Password Policy.

6.10 *JMH Group Software Licenses*

The JMH Group is part of a Microsoft corporate licensing program which provides employees with legal access to software required to perform their job roles. This process enables the JMH Group to monitor software usage and compliance. License key access should be kept to a minimum to ensure correct access to Company software. Any attempt to pass on license key information to 3rd parties or employees for personal use will result in disciplinary action.

6.11 Remote Access

It is the responsibility of all Company employees with remote access privileges to the Company network to ensure that their remote access connection is given the same consideration as the user's on-site connection to the Company.

Refer to Network Connection Policy for protocols and more information.

- Secure remote access must be strictly controlled
- Control will be enforced via password authentication or public/private keys with strong passphrases
- At no time, should any Company employee provide their login or email password to anyone else
- If a Company employee is connected to a non-Company network using a Company owned device, then a VPN solution should be used except for personal networks that are under the complete control of the user.
- All hosts that are connected to the Company internal networks via remote access must use the most up-to-date anti-virus software
- No personal devices should be connected to the Company network either directly or via remote access at any time

6.12 Firewalls and Malware

The Company understands that adequate and effective firewalls and protected gateways are one of the main and first lines of defence against breaches via the internet and internal networks.

We utilise configured firewalls and have anti-virus applications running on all computers, networks, and servers. The IT Service Desk is responsible for checking the log of all scans and for keeping these applications updated and compliant.

Systems are regularly scanned and assessed for unused and outdated software with the aim of reducing potential vulnerabilities and we routinely remove such software and services from our devices where applicable.

The IT Service Desk is also responsible for ensuring that the latest application and software updates and/or patches are downloaded and installed, keeping our security tools current and effective. Security software is reviewed and updated monthly, or sooner where updates or patches have been released.

7 Security Breach Management

7.1 Introduction

The Company's definition of a breach for the purposes of this and related documents, is a divergence from any standard operating procedure (SOP), which causes a failure to meet the required compliance standards as laid out by our own compliance program objectives and/or those of any regulatory body.

Compliance in this document means any area of business that is subject to rules, laws, or guidelines set out by a third party which are to be followed and which, when breached, could cause emotional, reputational, or financial damage to a third party.

7.2 Breach Management Approach

The Company has robust objectives and controls in place for preventing security breaches and for managing them if they do occur. Due to the nature of our business, the Company processes and stores a limited amount of personal information and confidential client data and as such, requires a structured and documented breach incident program to mitigate the impact of any breaches. Whilst we take every care with our systems, security, and information, risks still exist when using technology and being reliant on human intervention, necessitating defined measures and protocols for handling any breaches.

We carry out frequent risk assessments and gap analysis reports to ensure that our compliance processes, functions, and procedures are fit for purpose and that mitigating actions are in place where necessary. Should there be any compliance breaches, we are fully prepared to identify, investigate manage and mitigate with immediate effect and to reduce risks and impact.

The Company has the below objectives with regards to Breach Management:

- To maintain a robust set of compliance procedures which aim to mitigate against any risk and provide a compliant environment for trading and business activities
- To develop and implement compliance breach and risk assessment procedures that staff are aware of and can follow
- To ensure that any compliance breaches are reported to the correct regulatory bodies within the timeframes as set out in their code of practice or handbooks
- To use breach investigations and logs to assess the root cause of any breaches and to implement a full review to prevent further incidents from occurring

- To use the Data Breach Incident Investigation form for all breaches, regardless of severity so that any patterns in causes can be identified and corrected
- To comply with regulating bodies and laws on compliance breach methods, procedures, and controls
- To protect consumers, clients, and staff – including their data, information, and identity

Please refer to our Data Breach Policy & Procedures for further details.

8 Responsibilities

All information users within the Company are responsible for protecting and ensuring the security of the information to which they have access. Managers and staff are responsible for ensuring that all information in their direct work area is managed in conformance with this policy and any subsequent procedures or documents. Staff who act in breach of this policy, or who do not act to implement it, may be subject to disciplinary procedures.

The Company will ensure that staff do not attempt to gain access to information that is not necessary to hold, know, or process, and that restrictions and/or encryptions are in place for specific roles within the organisation relating to personal and/or sensitive information.