Contents

Change History			
Date	**Issue**	**Approved**	**Reason for Amendment**
25/03/2014	1	SN	First issue
22/01/2015	2	SN	Updated to reflect current practices and correct initial drafting errors
16/02/2016	3	SN	Update procedure to show restrictions are in place to prevent misuse of the computer systems.
28/06/2017	4	CH	Updated procedure to include required changes highlighted through the annual audit schedule.
01/02/2019	5	CH	Updated Clause 6.1 to include the newly chosen method of measuring the effectiveness of the procedure. Also fixed the numbering of the clauses so that it is clearer and in line with the contents section.
11/02/2019	6	SN	8.1.11 All unnecessary user accounts are promptly removed or disabled 8.1.12 Employee user accounts are disabled upon employment cessation 8.1.13. The auto-run from removable media feature is disabled, company-wide. 8.1.14. Employees are allocated data access privileges in accordance with the nature of their role within the business 8.2.4 Internet access to administration interfaces of all devices is disabled 8.4 Password Creation 8.5 Password Protection 10.3. All critical and security software patches must be installed within 14 days of release
01-10-19	7	CH	Add DSE Risk Assessment (MSF 203) to references.

Purpose

The purpose of this procedure is to define the responsibilities and activities involved in controlling the company's computer equipment and protecting its data.

Scope

This procedure embraces all the activities involved in the control and management of the company's IT systems.

Responsibility

The IT Manager is responsible for overseeing the implementation and maintenance of an efficient computerised service.

The IT Manager is responsible for the day to day running of the computer system and ensuring the requirements of this procedure are met.

References

- Document and Record Control MSP 002
- DSE Risk Assessment MSF 203
- Computer Software help files

Definitions

The computer network at Goody Demolition is essential to the day to day running of the business and is used 7 days a week to store and access a variety of both local and online information and to facilitate communication via email and telephone

DSE Risk Assessment: A specific risk assessment carried out for Display Screen Equipment Users, to ensure their work station is correctly set up and does not present additional Health and Safety risks in the performance of their work.

Work Station: An area set aside for the operation of a computer, this includes the computer equipment, accessories, chair, work surface and surrounding areas and activities.

Information Stored

- IT hardware audit results (see 1.2)
- A list of online resources relevant to any IT hardware including manuals, support access and warranty information
- Software licensing audit results
- Software licensing details including any usernames and passwords used to access online licensing repositories
- Software support access details
- Accountancy information ranging from purchase and sales invoices to internal accounts. No payment information is stored anywhere on the network
- Management information and statistics i.e. meeting minutes, procedure manuals and employee time sheets
- Emails (see 2)

Hardware	All hardware either related to or connected to the computer network i.e. servers, workstations, printers, scanners, monitors, pc peripherals and desk phones An audit of IT hardware is kept and updated automatically on a daily basis or where not appropriate, is maintained by the IT manager.
Software	Any computer software used to facilitate the daily operation of the business and is installed or otherwise located on the computer network in any way

Measurement of the process

6.1. The effectiveness of this procedure will be measured by the number of reported IT related problems. Measurement of this process will be in the form of a spreadsheet which collates the details of all problems identified. The spreadsheet will need to include: Date the problem was identified, description of the problem, action taken and the date of action being completed.

6.2. It will also be measured by the company's ability to process data efficiently and accurately to maintain operational performance.

General Requirements

7.1. A networked computer system is installed in the head office allowing all company data to be stored in a central location and shared across the network.

7.2. All requests for computer services up-date or addition to existing software shall be made direct to the IT Manager who will assess the need and cost of the change, liaise with the Accounts Manager and approve the change as necessary.

7.3. Computer system assistance is provided by the IT Manager, staff should contact the IT Manager directly to resolve issues.

7.4. The computer network is an essential part of the Company's Management System. It shall be maintained in good working order at all times and regularly revised to ensure its effectiveness

7.5. Hardware configuration of individual computers shall be under regular review to ensure they are capable to execute their specific tasks.

7.6. A system of preventive maintenance including virus protection software shall be operational to avoid premature failure whenever possible and repairs shall be rapidly effected should the need arise.

7.7. The stocks of computer and printer consumables shall be monitored and timely re-ordering made whenever the rate of consumption dictates.

7.8. Computer operators shall have adequate knowledge to operate specific computers safely and efficiently and additional training shall be given, as the need arises.

7.9. All Computer Operators shall complete a DSE Risk Assessment on an annual basis. This assessment shall also be repeated if new work station equipment is provided or if the workstation is moved to a different location (Please refer to Section 9 of MSP 010 for additional details and also the responsibility for organising the assessments for staff).

7.10. All anomalies shall be reported to the IT Manager or Operations Manager by the operator to permit rapid corrective actions to be effected.

7.11. All operators shall contact the IT Manager whenever additional information or assistance is required in performing their specific tasks.

7.12. Care shall be taken in the use of all computer equipment to prevent damage.

7.13. All employees are required to adhere to the company's IT Systems Use Policy which details the misuse and appropriate use of the computer system and telephone system. Certain types of websites and websites which flag up as dangerous (for example contain viruses) are blocked to prevent misuse or damage.

Security

8.1. Internal

8.1.1. All digital information is appropriately grouped and then stored in a partitioned area on the network

8.1.2. Each information partition is secured with a username and password and can only be accessed by designated employees

8.1.3. Employees can only access their individual email accounts and centrally assigned shared accounts

8.1.4. Employees email accounts are secured by a username and password combination

8.1.5. Appropriate workstation and server anti-malware software is installed on every system

8.1.6. All internet connections are automatically scanned for malware at the email gateway

8.1.7. All emails are scanned for malware at the email gateway.

8.1.8. Only required communication ports are open to the public internet from the Network Access Gateway.

8.1.9. Open communication ports from the Network Access Gateway are regularly reviewed for necessity.

8.1.10. Communication port access is reviewed and authorised by the IT Manager, Operations Manager and / or the Managing Director.

8.1.11. All unnecessary user accounts are promptly removed or disabled

8.1.12. Employee user accounts are disabled upon employment cessation

8.1.13. The auto-run from removable media feature is disabled, company-wide.

8.1.14. Employees are allocated data access privileges in accordance with the nature of their role within the business

8.2. Remote Access

8.2.1. Only designated employees are able to access the computer network remotely

8.2.2. Remote access is secured with a username and password combination

8.2.3. Remote access communication channels are encrypted between the end-users device and the network gateway server

8.2.4. Internet access to administration interfaces of all devices is disabled

8.3. IT use policy

8.3.1. All employees are subject to the IT Systems Use Policy

8.4. Password Creation

8.4.1. All user and admin passwords must be at least [8] characters in length. Longer passwords and passphrases are strongly encouraged.

8.4.2. Passwords must be completely unique, and not used for any other system, application, or personal account.

8.4.3. Default installation passwords must be changed immediately after installation is complete

8.5. Password Protection

8.5.1. Passwords must not be shared with anyone (including co-workers and supervisors), and must not be revealed or sent electronically.

8.5.2. Passwords shall not be written down or physically stored anywhere in the office.

8.5.3. When configuring password “hints,” do not hint at the format of your password (e.g., “postcode + middle name”)

8.5.4. User IDs and passwords must not be stored in an unencrypted format.

8.5.5. User IDs and passwords must not be scripted to enable automatic login.

8.5.6. "Remember Password" feature on websites and applications should not be used unless using a web browser under the context of an authorised user account.

8.5.7. All mobile devices that connect to the company network must be secured with a password and/or biometric authentication and must be configured to lock after 3 minutes of inactivity.

Backup

9.1. All data on the network is automatically mirrored to an off-site server and is automatically backed up twice daily: once at 07:00 and once at 12:00. The off-site server is then backed up overnight once per week for historical data retrieval.

9.2. Some data held on individual computers will not be backed up by the action described in 9.1 above. This data will be the responsibility of the data owner who will decide the frequency and need to make backups

9.3. The company I/T system should be restorable to a sufficient standard to allow the business to be operational within 24 hours.

Software

10.1. The company will hold sufficient software licences for the software used by its employees.

10.2. All Software discs will be stored digitally on the server and backed up in the regular backups. Where appropriate, originals will be destroyed.

10.3. All critical and security software patches must be installed within 14 days of release

Quality Checks

11.1. All data security assignments are reviewed periodically during management meetings to ensure employees have access to the information they require to perform their duties and to prevent unauthorised access to and potential leakage of sensitive information

11.2. IT use policy is periodically reviewed during management meetings to ensure it is up-to-date and relevant to the companies dynamic IT environment

11.3. The integrity of each backup is tested to ensure that data can be retrieved from it if the need arises

11.4. Regular malware scans are performed on every system to ensure the data and systems are not compromised

11.5. Business continuity plan periodically reviewed to ensure effectiveness

End of Life Disposal

12.1. All computer equipment should be disposed of in accordance with The Waste Electrical and Electronic Equipment (WEEE) Directive or made available for reuse.

12.2. Hard drives are removed and archived. If the need arises to destroy the hard drive they will be destroyed in accordance with HMG IA5 Standard.

12.3. Where possible spent printer cartridges and toners shall be disposed of via a recycling facility.

Disaster Recovery and Business Continuity

See business continuity plan