# Security and IT Policy

| | |
|---|---|
| **Document:** | Security and IT Policy |
| **Revision no:** | 3.3 |
| **Creation Date:** | 5th January 2016 |
| **Updated** | 16th July 2020 |
| **Status:** | Published |
| **Approved by:** | Andy Nash– Infrastructure Manager<br>Jeremy Pile – CTO<br>Andy Reeves – Data Protection Officer |
| **Signed:** | |
| **Next Review date:** | January 2020 |
| **Modified by:** | George Chapman – Security specialist |

Table of Contents

# 1. SECURITY AND IT POLICY

## 1.1 Information Security Objective

Company information is considered to be a critical and valuable asset to the Company. The objective of Information Security is to preserve:
**Confidentiality** – ensuring that information is accessible only to those authorised to have access.
**Integrity** – safeguarding the accuracy and completeness of information and processing methods.
**Availability** – ensuring that authorised users have access to information and associated assets when required.

The management of the Company is committed to, and fully supports, the goals and principles of IT security, and fully expects that this policy will adequately protect the Company's electronic information to a degree that is commensurate with the associated risks.

## 1.2 Document Ownership

Ownership of this document is assigned to the Information Security Group (ISG) who are responsible for its maintenance and review. They will instigate appropriate changes to the policies as and when circumstances dictate. Such circumstances could be, significant security incidents, newly identified vulnerabilities, changes to the organisational or technical infrastructure, cost and impact of existing policies on the Company's business and operating efficiency, technological changes etc.

## 1.3 Document Purpose

This document provides a framework for security for all Information Systems and Services in use throughout Muddy Boots Software Ltd (referred to as **the Company**). All other policies and procedures operate under the context of this policy. This policy describes how the Company protects its electronic information.

This document describes a set of controls, comprising policies, practices, procedures, organisational structures and software functions.

# 2. ORGANISATIONAL SECURITY

## 2.1 Management Structure

The Chief Executive, as Accountable Officer, has responsibility for Corporate Governance. Responsibility in relation to Information Governance has been delegated to Information Security group lead by the Data Protection Officer. The information security group consists of Data Protection Officer, Chief Technical Officer, Infrastructure Manager and Security Specialist(s).

## 2.2 Allocation of information security responsibilities

The Company identifies 6 distinct roles (i.e. types of employee), each of which is given responsibility for carrying out specific security procedures:

- Data Protection Officer
- Infrastructure Manager
- Security Specialist
- System Manager
- Line Manager
- Users.
- Information Asset Owner

### 2.2.1 Data Protection Officer

- Reports on company security to Board level
- Co-operate with the relevant regulatory authority (the ICO in the UK)
- Leads the Information Security Group
- Ensures safeguards are in place for Personal Data protection
- Ensures compliance with relevant legislation.

### 2.2.2 Infrastructure Manager

- Reports on IT security to the Information Security Group.
- Manages the Infrastructure and Security Teams
- Co-ordinates IT Security matters across the Company and acts as the central point of contact.
- Documents, implements, monitors and maintains the IT Security Policy and monitors its effectiveness.
- Provides guidance to System Managers and Information Owners in relation to their specific areas of responsibility.
- Ensures that risk assessments and security reviews are carried out, in consultation with users, as and when circumstances dictate.
- Ensures that agreed recommendations emerging from risk analyses are implemented.
- Collates and analyses reports of IT Security incidents and initiates appropriate action.

### 2.2.3 Security Specialist

- Daily operation of the security processes for the Company's IT infrastructure and computerised information systems
- Ensure security scans are completed across external and internal networks
- Monitors and maintains the company SIEM Solution.
- Promotes IT security awareness throughout the Company and helps to identify appropriate training for staff.
- Facilitates 3rd party security audits/penetrations tests as appropriate.

### 2.2.4 System Managers

Each Information System has an identified System Manager who is responsible, amongst other things, for aspects of security for that system. The key areas for which the System Manager has responsibility are:

- Controlling user access to the system by:
- Issuing passwords only to those authorised to have them.
- Ensuring that user access levels are appropriate to the job function.
- Ensuring that passwords are changed on a regular basis.
- Withdrawing passwords for officers who no longer require them or who are no longer in the post for which the password was issued.
- Monitoring to detect unauthorised activities.
- Developing and maintaining a Contingency Plan for the system.
- Safe-keeping software application documentation.
- Preparing and maintaining operating procedure manuals.
- Reporting both breaches of security and system vulnerabilities to the Security Team.
- Ensuring that the introduction of authorised changes to the system are thoroughly tested prior to implementation, and that the implications for the integrity of the system are carefully examined. Where appropriate, such changes should be undertaken in conjunction with the System manager and Infrastructure Manager.
- Testing and accepting new software released on behalf of the Company and in particular, ensuring that there is no risk to the integrity of the system.
- Monitoring system performance and assisting with capacity planning, in conjunction with the Infrastructure department.

- Ensuring third parties do not have access to information systems or the facility to access or copy data without appropriate authorisation and controls.

### 2.2.5 Line Managers

Line Managers in departments where Information Systems are in use are required to:

- Ensure staff have IT security awareness training.
- Ensure that all users of IT within their departments are aware of the existence of the IT Security Policy and that it has been read and understood.
- Ensure that the IT Security is implemented within their own department.
- Authorise levels of access to information systems that are appropriate to the job function.
- Ensure that all information assets are registered with the IT Service Desk

### 2.2.6 Users

The most common breaches of IT security are brought about by the actions of individual users. However secure users can also form one of our best defences. Users must therefore:

- Be aware they are personally accountable for their actions.
- Accept responsibility for the security of their Personal Computer (PC), laptop, PDA/smartphone, encrypted memory stick etc. and the information stored on it.
- Declare any personal interest in information or any other aspect of Information Technology which could lead to a conflict of interest.

### 2.2.7 Information Asset Owner

Information asset owners are senior individuals involved in running the relevant business. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why

The IAO role includes the following aspects

- Knows what information the asset holds, and what enters and leaves it and why
- keeps understanding of the asset and how it is used up to date
- approves and minimises transfers while achieving the business purpose
- approves arrangements so that information put onto removable media like discs or laptops is minimised and protected
- approves the disposal mechanisms for paper or electronic records from any asset
- Knows who has access and why, and ensures their use of it is monitored
- understands the organisation's policy on use of the information
- check that access provided is the minimum necessary to achieve the business purpose
- receives records of checks on use and assures self that they are being conducted
- Understands and addresses risks to the asset, and provides assurance to the Infrastructure Manager
- contribute to the organisation's risk assessment
- considers whether better use of the information could be made
- receives and logs requests from others for access
- ensures decisions and recording of authorisation on access are taken accordingly

## 2.2 Risk Assessment

Risk Assessment may be broken down into four main functions: -

The identification of the assets. The assets within the scope of the risk assessment should be checked against an Asset Register.

The evaluation of the impact of an adverse event (threat) on the assets. An event does not necessarily have to be a disaster in the normally understood sense, such as a fire. It can also be an event which simply prevents the system from operating for a period of time. This could be machine failure, operator error, and malicious interference;

The assessment of the likelihood of the adverse event occurring. There can be a tendency to underestimate the likelihood of an event occurring. Fire and malicious infiltration, such as hacking or burglary, could be likely, irrespective of the location of the assets

The identification of appropriate countermeasures to protect the asset and/or limit the damage caused by an event.

### 2.2.1 IT Risk Management

In order to meet the stated objectives of Muddy Boots risk management, we shall execute a strategy to "identify", "minimise" and "manage" the risks to their information assets through the implementation of a Risk Treatment Plan, Testing and Remediation activities through the implementation and oversight of information security policies and procedures.

Muddy Boots Risk Treatment metrics are as follows and are held within our risk management software and managed via regular ISG (Information Security Group) meetings

| | | | | |
|---|---|---|---|---|
| **Likelihood** | High<br>occurs more than every 3 months | **Risk Level 3** | **Risk Level 6** | **Risk Level 9** |
| | Medium<br>Occurs between 3 months and 2 years | **Risk Level 2** | **Risk Level 4** | **Risk Level 6** |
| | Low<br>Occurs less than every 2 years | **Risk Level 1** | **Risk Level 2** | **Risk Level 3** |
| | | Low | Medium | High |
| | | **Impact** | | |

| **Impact Values** | **Low** | **Medium** | **High** |
|---|---|---|---|
| Financial | < £10k | £10k-£100k | >£100k |
| Reputational impact | | | |
| Loss of data | Customer unhappiness | Customer refusing recommend | Loss of customer<br>Regulator activity |
| Quality of software | Customer unhappiness | Customer refusing recommend | Loss of customer |
| Reliability of service i.e. | Service unavailable < 1 hour per day | Service unavailable 1 day | Service unavailable +1 day |

| | | | |
|---|---|---|---|
| unplanned downtime | | | |
| Client expectation (functionality of software) | Customer unhappiness | Customer refusing recommend | Loss of customer |
| Confidentiality breach | Customer unhappiness | Customer refusing recommend | Loss of customer<br>Regulator activity |

| | | |
|---|---|---|
| Risk Calculation | Risk = Impact * Likelihood | |
| Risk Acceptance | Risks at level 2 or less are acceptable | |
| | Risks above level 2 are to be treated | |
| | Risks at level 2 or less may be treated if deemed appropriate by management | |

Having assessed the levels of risk, risk management identifies the protective measures that could be applied to reduce the risks to acceptable levels.

Possible actions include:

a) Applying appropriate controls to treat the risk
b) Knowingly and objectively accept risks, providing they clearly meet the Company policies and the criteria for accepting risk.
c) Terminate the activity giving rise to the risk.
d) Transfer the associated business risks to other parties, e.g. suppliers.

### 2.3 Confidentiality and Data Security Agreements

Confidentiality is included in all employee contracts, customer contracts and suppliers/partners should have mutual non-disclosure agreements in place.

### 2.4 Contact with authorities

Appropriate contacts with law enforcement authorities, regulatory bodies, information service providers and telecommunications operators are maintained to ensure that appropriate action can be taken quickly and advice can be obtained in the event of a security incident.

General Data Protection Regulation (GDPR) Statement

Privacy Policy

Disclosure Policy

### 2.5 Contact with special interest groups

Muddy Boots may contact specialist authorities for advice when needed

### 2.6 Independent review of information security

Muddy Boots is audited externally at least annually; we have attained HMG Cyber Essentials Security Plus status and align ourselves with ISO27001 practices.

### 2.7 User responsibilities

All Muddy Boot's employee's and users have a responsibility to follow the company Information Security Processes and policies as published.

## 3. ASSET ACCOUNTABILITY AND CONTROL

All IT assets within the company (PCs, laptops, smartphones, tablets etc.) should be listed on the company register of assets.

### 3.1 Procurement

Procurement of IT equipment, software and services is co-ordinated by the Infrastructure Department to ensure alignment with technical standards.

### 3.2 Disposal

The Infrastructure department identify and organize the disposal of IT equipment.

Equipment that has been assessed as of no further use to the Company is disposed following our process which ensures:

- Alignment with WEEE Guidance.
- All data is securely wiped

### 3.4 IT Asset Register

The IT Asset Registers will store details (including location) of all servers, PCs, software and peripherals (printers, scanners etc.). Each PC and server device have a designated owner/user and all peripherals are linked to a specific PC/server, thereby linking these to the owner/user.

The Infrastructure Department is responsible for creating and maintaining the digital systems that manage the IT devices on the register. Finance department maintain a full company asset register.

### 3.5 Tracking movements of equipment

IT equipment may be moved for any of the following reasons:

- Obsolete or old equipment may be replaced with new;
- User department moving office/building; or
- A change in user requirements.

When this occurs, the register will be updated

### 3.6 Information Classification Policy

It is critical for the Company to set the standard for the protection of information assets from unauthorized access and compromise or disclosure. Accordingly, the Company has adopted this information classification policy to help manage and protect its information assets.

- Company Managers or information 'owners' shall be responsible for assigning classifications to information assets according to the standard information classification system presented below. ('Owners" have approved management responsibility. 'Owners' do not have property rights.)
- Where practicable, the information category shall be embedded in the information itself.
- All Company associates shall be guided by the information category in their security-related handling of Company information.
- Information assets that are not marked with a classification are by default set to restricted.

All Company information and all information entrusted to the Company from third parties falls into one of four classifications in the table below, presented in order of increasing sensitivity.

| **Information Category** | **Description** | **Examples** |
|---|---|---|
| Public | Information is not confidential and can be made public without any implications for Muddy Boots Software. Loss of availability due to system downtime is an acceptable risk. Integrity is important but not vital. | • Product brochures widely distributed.<br>• Information widely available in the public domain, including publicly available Company web site areas.<br>• Sample downloads of Company software that is for sale.<br>• Financial reports required by regulatory authorities.<br>• Newsletters for external transmission. |
| Restricted | Information is restricted to management approved internal access and protected from external access. Unauthorized access could influence Company's operational effectiveness, cause an important financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence. Information integrity is vital. | • Passwords and information on corporate security procedures.<br>• Know-how used to process client information.<br>• Standard Operating Procedures used in all parts of Muddy Boots Software's business.<br>• All Company-developed software code, whether used internally or sold to clients. |
| Customer Confidential | Information received from customers in any form for processing in production by Muddy Boots Software. The original copy of such information must not be changed in any way without written permission from the client. The highest possible levels of integrity, confidentiality, and restricted availability are vital. | • Customer media.<br>• Electronic transmissions from clients.<br>• Product information generated for the customer by Muddy Boots Software production activities as specified by the customer. |
| PII or PCI | Personally, Identifiable Information (PII) or payment data such as credit card details covered by Payment Card Industry Data Security Standard and under GDPR | • Individuals name and address, credit card number or any additional personally identifiable data set out under GDPR regulations coming in to force in May 2018. |

| | | |
|---|---|---|
| Company Confidential | Information collected and used by Muddy Boots Software in the conduct of its business to employ people, to log and fulfil client orders, and to manage all aspects of corporate finance.<br>Access to this information is very restricted within the company. The highest possible levels of integrity, confidentiality, and restricted availability are vital. Again, where personally identifiable data is concerned, this comes under GDPR regulations, applicable from May 2018. | • Salaries and other personnel data.<br>• Accounting data and internal financial reports.<br>• Confidential customer business data and confidential contracts.<br>• Non-disclosure agreements with clients\vendors.<br>• Company business plans. |

### 3.7 Configuration Management

- Installation of new software or hardware, or changes to configurations, is only permitted provided appropriate licensing arrangements or other similar conditions of the supplier are met.

### 3.8 Device Management

All Muddy Boots mobile devices must be managed by the mobile devices management tool. This should ensure compliance with our standards as well as providing capability to decommission/remote wipe as required

## 4. HUMAN RESOURCES SECURITY

The HR Department participates in the information security of the company by ensuring contracts, policies and procedures are maintained to cover the below:

- Employee screening
- Employee Confidentiality
- Employee Data Protection
- Employee Privacy
- Employee Social Media
- Employee Termination/Change of employment

These are viewable in the company HR Portal

## 5. PHYSICAL AND ENVIRONMENTAL SECURITY

### 5.1 Secure areas

Data Centre

Our staging and live customer data are located on Company owned equipment hosted with Six Degrees Group in their Birmingham based Tier-4 aligned data centre. This data centre is protected with a steel barred fence, CCTV and 24/7 onsite security, with dedicated Racks protected by a locked door code. The datacentre is also protected from environmental threats by rack UPS and generator, with air conditioning, fire suppression and humidity sensors. They are an ISO27001 accredited organisation, and fully compliant with GDPR regulations.

Head Office

Our development, test and office systems are located at our head office near Ross-on-Wye. This location also acts as the remote DR location should the data centre become unavailable for any reason. The computer room is located in the basement with no windows behind a double locked steel door. When the office is empty the office is protected by an alarm linked to the local police. The computer room is also protected from environmental threats by rack UPSs and generator, with air conditioning and fire sensors.

### 5.1.1 Securing offices, rooms and facilities

Please refer to section 5.3 – General Controls for Securing of general offices.

### 5.1.2 Working in secure areas

Only authorized individuals allowed to work in the secure areas.
Access at DC is controlled by proximity card authorized access given by 6DG security based on the portal request from authorized the Company's management.
Access to Head Office Computer room is secured to only the Infrastructure team by physical keys

### 5.1.2 Data Communications Equipment

All major data communications cabinets/end points are secured in lockable cabinets and at both Live and DR sites are located in the secured restricted access server room.

### 5.1.3 Desktop Equipment

Please refer to section 5.3 – General Controls for Securing of general offices.

### 5.1.4 Physical entry controls

Data Centre

- Advanced authorized access requested by authorised Company management
- Met at the gate and ID check with passport or driving license only
- Sign in, photo taken, and access badge allocated once secondary check on ID.
- Access from reception to centre is via a one at a time with access card weight measured. Level of access card with either allow access only to meeting rooms or to specific floor and datacentre level with the Company's cage.
- Access to pod is via proximity access card.
- Access to cabinet is protected by combination lock

Head Office

- Sign in to visitor's register, email or SMS is sent to member of staff to collect visitor from reception.
- Visitor card printed out and must be worn at all time.
  Escorted at all times by the Company employee.
- Secure areas are locked at all times and only accessible by authorized staff; Server and boiler room.
- Outside of working hours the office is protected by security alarm controlled by authorized members of staff.

## 5.2 Equipment Security

Equipment is physically protected from security threats and environmental hazards to prevent loss, damage or compromise of assets and interruption to the Company's activities so far as is possible. All company computers have encrypted hard drives, with remote wipe capability.

### 5.2.1 Equipment siting and protection

All major Computer Rooms are protected by fire alarms and fire extinguishing systems. All Computer Rooms are air conditioned and temperature controlled. Eating, drinking and smoking are not permitted in these areas.
IT and information processing equipment should be sited in a way that affords it the best possible protection from security threats and environmental hazards.

### 5.2.2 Power supplies

Critical hardware such as servers and communications equipment is protected from power supply failure by the use of uninterruptible power supplies (UPS), which offers battery-based backup power. All UPSs are on essential services electric supply, which means that power will be restored within the shortest possible time following power failure, from a local emergency generator. Consequently, the combined use of UPS and emergency generator ensures that essential hardware is protected from failure due to power outages.

### 5.2.3 Cabling security

CAT5e/CAT6 network cabling is used throughout the Company's Domain.

Patch panels are located in the server room and only accessible by the Infrastructure team. Please see section 7.7.10, which states no non-Company device is permitted to be connect to the domain via cable or Wi-Fi.

Cables are colour coordinated and labelled.

### 5.2.4 Equipment maintenance

Support agreements are in place to maintain our environment and external contracts with hardware and software providers. Any external contractor is accompanied onsite by an authorised Company employee.

### 5.2.5 Security of equipment off-premises

All company laptops have full hard disk encryption and use the Company's VPN to connect to the Company's domain. Users are responsible for the protection of portable/home based equipment and any data stored on it. Staff are required to use the VPN when accessing any company assets outside of our domain/Firewall.

### 5.2.6 Secure disposal or re-use of equipment

As described in section 3.2 all equipment identified for disposal or reuse should be held in secure storage until it is redeployed or disposed of.

## 5.3 General controls

### 5.3.1 Clear desk and clear screen policy

Clear screen

- All computers/mobile devices are either logged out or manually locked whilst not attended. Computers will lock after a designated period of keyboard or mouse inactivity which is centrally controlled by group policy.
- Computer screens should be angled away from the view of unauthorised persons. Privacy screens have been implemented for highly confidential areas such as HR and Finance.

Clear desk

- Where practically possible, paper and computer media should be stored in suitable locked safes, cabinets or other forms of security furniture when not in use, especially outside working hours.
- Where lockable safes, filing cabinets, drawers, cupboards etc. are not available, office/room doors must be locked if left unattended. At the end of each session all sensitive information should be removed from the work place and stored in a locked area. This includes all client/staff identifiable information, as well as business critical information such as salaries and contracts.
- Sensitive or classified information, when printed, should be cleared from printers immediately.
- Before a client enters a meeting room all confidential information should be removed from view, including but not restricted to flipcharts, whiteboards, computer screens, contracts, papers etc.
- It is good practice to lock all office areas when they are not in use.
- The reception desk can be particularly vulnerable to visitors. This area should be kept as clear as possible at all times; in particular client/staff records or any other identifiable information should not be held on the desk within reach/sight of visitors.
- It is also worth noting that information left on desks is also more likely to be damaged or destroyed in a disaster such as fire, flood or explosion.

- Paper records no longer required should be shredded and disposed of immediately.

### 5.3.2 Delivery and loading areas

Data Centre
Dedicated loading areas at DC, access only allowed by pre- authorized requests and named individuals attending site and details of delivery confirmed. This requires a formal document submission and submission of details relating to any vehicle accessing the data centre.

Head Office
Loading area at Head office is via main building entry and secured by Reception. Additional loading area to rear of building – the Company’s employee will unlock and supervise the delivery into the building.

## 6. COMMUNICATIONS AND OPERATIONS MANAGEMENT

## 6.1 Operational procedures and responsibilities

This section covers responsibilities and procedures for the management and operation of all information processing facilities.

### 6.1.1 Documented operating procedures

System Managers are responsible for the preparation and maintenance of operating procedure manuals.

### 6.1.2 Operational change control

Change control procedures are in place and recorded in support systems. Notifications are sent to all staff as and when any major changes are put in place.

### 6.1.3 Incident management procedures

Refer to Section 9.

### 6.1.4 Segregation of duties

Where application software permits, formalised segregation of user duties is in place as a means of reducing risk of accidental or deliberate system misuse. This is particularly important for financial systems.

Muddy Boots will utilise activity logs, audit trails, and management supervision as a means of detecting system misuse or fraud as per procedure manuals and within constraints of system design.

### 6.1.5 External facilities management

In cases where systems are hosted in the supplier's environment the Company should be in line with agreed standards and processes. Similarly, systems hosted in the data centres are controlled and managed by the Infrastructure team.

## 6.2 System planning and acceptance

In order to ensure the availability of adequate capacity and resources, and thereby minimise the risk of system failures, advance planning and preparation is undertaken.

### 6.2.1 Capacity planning

The performance of the Company's physical / virtual servers and data communications is continually reviewed via event management. Appropriate action as BAU is implemented to adjust capacity accordingly within tolerances.

Strategic Capacity planning reports are updated on a regular basis including projects and the projected capacity required; this ensures our customer and company growth is anticipated and planned for.

#### 6.2.2 System acceptance

System acceptance criteria for new Information Systems (or upgrades to existing systems) are included in Project Plans and typically provide for security and user authentication controls, performance and capacity requirements, error recovery and contingencies, user training, and pre-deployment system testing (including verification of the backup process).

### 6.3 Protection against malicious software

Precautions are in place to prevent and detect the introduction of malicious software. This includes the use of multiple anti-virus and scanning applications across both the network and individual machines connected to our networks.

#### 6.3.1 Anti-Virus software

All company laptops/PC and servers will have up-to-date anti-virus installed and maintained. This will be configured to alert centrally so as to be monitored by Infrastructure and security teams.

Rules are in place to quarantine and auto fix, then track for 7 days to ensure it has not tried to install again. An incident ticket is raised and the IT Service Desk contacts the user of the infected PC and takes appropriate action.

Staff should also contact the IT Service Desk immediately if a virus is detected on their system.

All detected incidents are reported to the security team

### 6.4 Housekeeping

In order to maintain the integrity and availability of information processing services, routine procedures are established for taking back-up copies of data and logging events and faults.

#### 6.4.1 Information backup

All data servers located in the Company’s Data Centres are backed up on an appropriate cycle with hourly recovery points taken and replicated on an hourly schedule to secure offsite storage.

Work stored on desktop systems is the responsibility of the user; all documents should be saved to the Company’s secure SharePoint site or to multi factor authenticated Microsoft OneDrive accounts.

#### 6.4.2 Fault logging

Users are required to contact the IT Service Desk by email/telephone to report any faults or problems that they experience, whether hardware or software related. The IT Service Desk staff will advise the user of the solution to their problem if possible, or alternatively refer the problem to others. All faults are logged on the IT Service Desk system.

### 6.5 Media handling and security

This policy is to ensure that Information storage media must be managed, controlled, moved and disposed of in such a way that the information content is not compromised. Personal media such as USB devices should not be used, brought in to the offices or connected to any MB device without prior consent. This includes BYOD mobile devices which should be charged from mains chargers and not from the USB port on company assets.

#### 6.5.1 Management of removable computer media (memory sticks, DVDs/CDs, PDAs etc.)

Computer media with sensitive or confidential information are stored in a suitable locked container when not in use. Staff are not permitted to take unencrypted removable media off the Company's premises, unless specifically authorised. Physical media transfer of data must be encrypted, and password protected. In case of transport by post, the parcel/letter must be sent recorded requiring a signature at the recipient's end.

#### 6.5.2 IOT and BYOD Device Policy

Staff members are reminded that no IOT device (Wi-Fi Enabled device) should be brought in to the office and/or connected to our company network without consent. This includes all mobile phones, that are not company controlled or authorised, tablet devices, Wi-Fi enabled IOT devices such as kettles, light bulbs etc. All of these can pose a significant threat to the company if they were to be compromised.

Any new devices introduced to our network can only be done so with Security approval.

Staff bringing in their own devices are permitted to connect these to our guest networks.

### 6.6 Disposal of media

Users are advised that unwanted disks, removable media magnetic tapes, CDs, printouts, and other sensitive documents must be disposed of securely and safely, to minimise the risk of sensitive information being disclosed to outside persons.

The Company provides a complete physical disposal programme for all media containing sensitive data [secure shredding] as necessary. Documents and printouts containing sensitive information are shredded.

### 6.7 Information handling procedures

Procedures for the handling, storage and disposal of information have been established to protect such information from unauthorised disclosure or misuse in the following sections.

### 6.8 Security of system documentation

The safe keeping of application software documentation (e.g. user manuals, training manuals, and procedures) is the responsibility of the System Manager. Infrastructure documentation is the responsibility of the Infrastructure Department.

### 6.9 Internet usage policy

This Internet Usage Policy applies to all employees of the Company who have access to computers and the Internet to be used in the performance of their work. Violation of these policies could result in disciplinary and/or legal action leading up to and including termination of employment.

### 6.9.1 Computer, email and internet usage

- Company employees are expected to use the Internet responsibly and productively. Internet access is limited to job-related activities only and personal use is restricted to authorised breaks.
- Job-related activities include research and educational tasks that may be found via the Internet that would help in an employee's role
- All Internet data that is composed, transmitted and/or received by the Company computer systems is considered to belong to the Company and is recognized as part of its official data. It is therefore subject to disclosure for legal reasons or to other appropriate third parties.
- The equipment, services and technology used to access the Internet are the property of the Company and the Company reserves the right to monitor Internet traffic and monitor and access data that is composed, sent or received through its online connections
- Emails sent via the Company email system should not contain content that is deemed to be offensive. This includes, though is not restricted to, the use of vulgar or harassing language/images
- All sites and downloads may be monitored and/or blocked by the Company if they are deemed to be harmful and/or not productive to business
- The installation of software such as non-company standard instant messaging technology is strictly prohibited.
- Personal email mailboxes are not accessible by any other member of staff unless specifically authorised by Infrastructure and senior management.
- Emails are archived

### 6.9.2 Unacceptable use of the internet by employees includes, but is not limited to:

- Any illegal behaviour
- Sending or posting discriminatory, harassing, or threatening messages or images on the Internet or via the Company email service
- Sharing confidential material, trade secrets, or proprietary information outside of the organization
- Sending or posting information that is defamatory to the Company, its products/services, colleagues and/or customers
- Introducing malicious software onto the Company network and/or jeopardizing the security of the organization's electronic communications systems
- Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities
- Passing off personal views as representing those of the organization
- If an employee is unsure about what constituted acceptable Internet usage, then he/she should ask his/her line manager for further guidance and clarification
- All terms and conditions as stated in this document are applicable to all users of the Company network and Internet connection. All terms and conditions as stated in this document reflect an agreement of all parties and should be governed and interpreted in accordance with the policies and procedures mentioned above. Any user violating these policies is subject to disciplinary actions deemed appropriate by the Company.

### 6.10 Information security in project management

All Company Software projects must do the following:

- Include security objectives in overall project objectives.
- Include security specifications in your project description.
- Perform a risk assessment specifically for the project you are to undertake.
- Make sure security rules/technology are included in all the steps/tasks of the project.
- Test if the project deliverables are compliant with security specifications

## 7. ACCESS CONTROL

### 7.1 User access management

To prevent unauthorised access to information systems, procedures must be in place to control the allocation of access rights.

#### 7.1.1 New Starter and Employee registration

Requests for all new starters must follow the appropriate process which is triggered by the line manager contacting the IT helpdesk after authorisation from HR.

#### 7.1.2 User privilege management

An essential element of ensuring that the security of the Company's IT Systems is maintained is to exercise control over user accounts. This function is the responsibility of the System Manager. A System Manager is identified with each application, including those that are hosted by other organisations.

While each system has its own unique access control mechanism, and some System Managers have specific procedures the general principles that are applied to all systems are:

1) Each system should:
   a) Permit access to a user only on entry of a legitimate user name (UserID) and password.
   b) Allow the system manager to restrict user access e.g. to different parts of the system or to view only, view + update, view + update + delete.
   c) Permit the System Manager to control permissions i.e. add or disable user accounts and set up/amend user profiles. System Managers should identify any system shortcomings in this regard and notify the Infrastructure Manager who will undertake a risk assessment.
   d) System Managers should adopt a logical approach to the allocation of usernames. This will enable users to be easily identified, for example, on reports.
2) Users should be able to access only those parts of the system that they require to do their job and in which they have been trained.
3) The System Manager should hold a log showing all those who have been allocated a user account. The log should contain the user name, designation, department, contact details and the user profile. The user profile should provide details of access levels given/removed and reviews undertaken, together with relevant dates.
4) Line Managers are responsible for notifying System Managers when staff changes or role changes within their departments require new accounts to be set up, accounts to be removed or levels of access to be

altered. System Managers should implement a process that clearly identifies that requests are authorised and instigated. Line Managers should not pass usernames and passwords from one post-holder to another.

5) System Managers in conjunction with the Infrastructure Manager should undertake a systematic review of accounts and user profiles with managers on a regular basis, at least annually, to ensure that current access levels are still appropriate.
6) System Managers should monitor accounts that have not been activated for a pre-set period and liaise with managers as to the appropriate course of action.
7) In some cases, it may be appropriate to set up an account with username and password for use by staff who work in the Company on a very short-term basis (typically 1 day) e.g. Agency. Such accounts should have a very limited level of access to the system.
8) System Managers and Infrastructure monitor failed log-in attempts. Alerts are automatically emailed to the IT Service desk to be actioned.
9) When training users, System Managers should reinforce the principle that usernames and passwords must not be shared.

## 7.2 Password Policy

All passwords should meet the below policy which is based on industry leading guidelines including sources such as NIST & NCSC. This policy should apply to any authentication system under Muddy Boots Control or any accounts created by its employee's e.g. internal active directory, our developed applications and accounts on third party services.

**Suggestion:**

We want your passwords easy to remember and hard to guess. Try to use random phrases/sentences made up of at least 3 words with no logical association. This has been proven to be hard to guess but easy to remember therefore providing a good balance of protection and usability.

**Password rotation:**
Password rotation should not be forced on a schedule but instead users should focus on having easy to remember hard to guess passwords. Passwords should be changed if at any point you feel this has been compromised or if you are advised to do so in response to an incident.

**Minimum Password age: 1 day**
This is the minimum time a user must have a password before they can change it. This means once you change a password you cannot change it back to a previously used one.

**Maximum Password age: N/A**
This is the maximum password age, passwords are to be changed if a breach is suspected.

**Password history: 24 passwords**

How many passwords are remembered to stop users repeating them.

**Password storage:**

Passwords should be stored using strong non-reversible encryption and storage outside of the authentication system should be avoided.
Avoid storing your password in browsers etc. using a memorable, non-expiring password should remove this need and help ensure your password isn't stored insecurely.

**Minimum Password length: 8 characters**
This is the minimum number of characters required for a password. This can be made up of alphanumeric and/or symbols.

**Maximum Password length: 64 characters**
This is the maximum number of characters a password can be.

**Account lock out**
Authentication systems should lock out the account in the advent of multiple incorrect password attempts. Exact configuration may vary due to sensitivity and appropriateness but at the very minimum should be the below:
Attempts to cause lock out: 5
Lock out duration: 30 minutes

**Password discoverability:**

Passwords should avoid using easily guessable/discoverable information. This includes but is not limited to:

- Personal information (Name, Data of birth, Children's/Pet's name, favourite sports team etc.)
- Common passwords (Password, Password1, password, 12345678, qwerty, football etc.)

**Password disclosure:**

Never tell anyone (including those in authority such as IT/Security, Managers) your password. Only enter it into the system if you are confident it is the correct system. If you ever feel like your password has been compromised change it and report it to security ASAP.

### 7.2.1 Screen time-out

On Windows-based PCs, password protected screen savers are automatically activated after an inactivity period of no greater than 15 minutes.

### 7.2.2 Password Manager Usage

On all systems it is recommended you use an encrypted password manager, should you manage or utilise more than two online or offline accounts relating to Muddy Boots in any way. (This does not include the account you login to your workstation/desktop/laptop with). Please see below for a list of recommended password managers.

1. Keepass

2. Dashlane

### 7.2.3 Single Sign On Solutions for MB Employees

We must use Muddy Boots Microsoft Single Sign on solution for all access to all business systems and services. This will mean your first.last@muddyboots.com account that you login to your workstation with should be how you authentication with Muddy Boots systems e.g. Cezanne, Confluence, Zendesk, TFS etc.
Any new business systems being purchased/rolled out should include the requirement for this single sign on/federated authentication.

Business systems that are exceptions to this should receive prior authorisation and be managed as a risk.

Where employees require to sign up for another service outside of Muddy Boots business systems but with their work email e.g. customer's portal, GitHub etc. choosing sign in with a Microsoft account should allow you to use your work credentials. If this is not possible a unique and secure password must be used.

### 7.2.4 Single Sign On Solutions for Customers

Our customers and any MB Employees needing to use/perform tests on our application, must use our Greenlight single sign on solution (where this is deployed).
This single sign on solution allows for the users to authenticate across all MB Customer Services and Solutions using the same account. i.e. GLGM and GLSA.
It is supported for customers to use federated authentication provided this is requested by a trusted contact at their end and that this federation is linked to our Greenlight Single Sign on solution.

### 7.2.5 Multi Factor Authentication

Multifactor authentication is mandatory in the Muddy Boots Single Sign on for all employees.

Where systems cannot be setup using the single sign on solution, multi-factor authentication should be setup within that solution where available.

## 7.3 User authentication for external connections

Staff may obtain external access to systems using a company approved and managed authentication system. Applications for this facility are made via the Company's IT Service desk.

External organisations providing remote system support obtain access through the same approved and managed authentication system and applications for this arrangement must be approved by Security team.

Remote access to the Company's systems via VPN is automatically terminated after a predefined period of inactivity.

### 7.3.1 Security of third party access and contracts with third parties.

Access to Information Systems by third parties must be carefully controlled to maintain their security. Complimentary contracts and additional controls should be in place for data sharing.
Where possible, outside contractors are issued unique time expired user IDs for on-site use and are carefully controlled in terms of permissions set in the User ID to restrict access to those parts of the system that are strictly necessary.

Remote access by third parties to the systems is occasionally required, usually to provide remote support for specific systems or applications. In such circumstances, access is managed and controlled by the Infrastructure department, as the entry point by the third party into the Company's systems.

Consequently, all issues relating to authorisation, authentication, firewalls and encryption are handled by Infrastructure department. Details of how to progress a request for 3rd party remote access should be addressed to the Security Team in the first instance; an NDA is requested, and authorisation approved or denied.

Management shall nominate a suitable Muddy Boots owner for each business function/process outsourced. The owner, with help from the Muddy Boots contract negotiator and the Infrastructure Manager, shall assess the risks before the function/process is outsourced, using Muddy Boots standard risk assessment processes.

In relation to outsourcing, specifically, the risk assessment shall take due account of the following

- Nature of logical and physical access to Muddy Boots information assets and facilities required by the outsourcer to fulfil the contract;

- Sensitivity, volume and value of any information assets involved;
- Commercial risks such as the possibility of the outsourcer's business failing completely, or of them failing to meet agreed service levels or providing services to Muddy Boot's competitors where this might create conflicts of interest; and
- Security and commercial controls known to be currently employed by Muddy Boots as outlined here and in the ISMS and/or by the outsourcer
- GDPR Regulations

The result of the risk assessment shall be presented to management for approval prior to signing the outsourcing contract. Management shall decide if Muddy Boots will benefit overall by outsourcing the function to the outsourcer, taking into account both the commercial and information security aspects. If the risks involved are high and the commercial benefits are marginal (e.g. if the controls necessary to manage the risks are too costly), the function shall not be outsourced.

A formal contract between Muddy Boots' and the outsourcer shall exist to protect both parties. The contract shall clearly define the types of information exchanged and the purpose for so doing. It will be compliant with GDPR regulations

If the information being exchanged is sensitive, a binding confidentiality agreement shall be in place between Muddy Boots' and the outsourcer, whether as part of the outsource contract itself or a separate non-disclosure agreement (which may be required before the main contract is negotiated).
Information shall be classified and controlled in according with Muddy Boots' IT and Security.

Any information received by Muddy Boots' from the outsourcer which is bound by the contract or confidentiality agreement shall be protected by appropriate classification and labelling.
Upon termination of the contract, the confidentiality arrangements shall be revisited to determine whether confidentiality has to be extended beyond the tenure of the contract.

All contracts shall be submitted to the Legal team for accurate content, language and presentation, including:

Legal, regulatory and other third-party obligations such as data protection/privacy laws, money laundering/GDPR etc.

Information security obligations and controls covered in our EULA and Legal terms and conditions outlined at en.muddyboots.com

In order to prevent unauthorized access to Muddy Boots' information assets by the outsourcer or sub-contractors, suitable security controls are required as outlined in this section. The details depend on the nature of the information assets and the associated risks, implying the need to assess the risks and design a suitable controls architecture.

**Technical access and system controls shall include**

- User identification and authentication using MFA
- Authorization of access, generally through the assignment of users to defined user roles having appropriate logical access rights and controls;
- Data encryption in accordance with Muddy Boot's encryption policies and standards defining algorithms, key lengths, key management and escrow etc.
- Accounting/audit logging of access checks, plus alarms/alerts for attempted access violations where applicable.
- Pseudonymisation and encryption of personal data in compliance with GDPR
- The ability to ensure ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data

- The ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident in compliance with our DR and backup policies contained herein.
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of all data processing and storage.

If parts of contracted systems or IT infrastructure are to be hosted at a third-party data centre, the data centre operator shall ensure that Muddy Boots' assets are both physically and logically isolated from other systems.

Muddy Boots' shall ensure that all information assets handed over to the outsourcer during the course of the contract (plus any copies made thereafter, including backups and archives) are duly retrieved or destroyed at the appropriate point on or before termination of the contract. In the case of highly classified information assets, this normally requires the use of a schedule or register and a process whereby the outsourcer formally accepts accountability for the assets at the point of hand-over.

If Muddy Boots' has outsourced a business function to an outsourcer based at a different location, it may request to audit the outsourcer's physical premises periodically for compliance to Muddy Boots' security policies, ensuring that it meets the requirements defined in the contract and are compliant with GDPR.

Special consideration must be given to the ramifications of transferring information between countries or jurisdictions, particularly where privacy and similar laws may conflict. GDPR will be the overriding legislation to which Muddy Boots will comply. Muddy Boots will seek qualified legal advice as a matter of course for any additional clarification where data transfers outside of the EU are required.

#### 7.3.4 Access Control Lists

Access Control Lists are used to control both in-bound and out-bound network traffic. These lists are maintained by the Infrastructure team.

#### 7.3.3 Use of Network Services

Access to network services is granted only to users who enter an authenticated username and password and is regularly reviewed and updated. We also implement a multi factor authentication process for access to any data critical systems.

### 7.4 Operating system access control

In order to maintain the security of operating systems only qualified IT staff have administrative privileges on desktop and server systems. This includes developers as well as Infrastructure support staff.

#### 7.4.1 User identification and authentication

Users are issued with unique user names for their personal and sole use (Refer to Section 7.1.1). The user name is validated by the password and then via multi-factor authentication where needed.

#### 7.4.2 Removal of access rights

When a member of staff or contractor leaves the organisation, their access rights to all information systems must be removed immediately. This will prevent unauthorised access and maintain accountability.

Where a member of staff or contractor moves to another post, their access rights should be reviewed and amended to reflect only the needs of the new post. This prevents authorisation creep and maintains the concept of least privilege.

## 7.5 Application access control

Security facilities are used to restrict access and prevent unauthorised access to information held within company systems.  (Refer to Section 7.1.2).

### 7.5.1 Information access restriction

Data stored on Windows-based systems residing on the network, are restricted by the read/update/delete permissions inherent in the users account.
Data stored on Windows PC/Laptop drives are restricted by the Windows User account permissions
Sensitive/confidential information should not be stored on the internal drive of IT equipment unless appropriate security measures have been applied. Laptops must have a fully encrypted [FDE] internal hard disk which must be encrypted using Bitlocker.

### 7.5.2 Sensitive system isolation

If data is particularly sensitive, it is completely isolated and secured using encryption techniques.

## 7.6 Monitoring system access and use

Where possible, systems are monitored to detect unauthorised activities.

### 7.6.1 Event logging

Security Audit Logging is activated on most PCs, and servers have security audit logging switched on to automatically record events such as failed logon attempts.   These logs are centrally gathered into the SIEM an immutable format.

### 7.6.2 Monitoring system use

All Windows server event logs are checked during the monthly server maintenance routines.  Network monitoring software automatically sends alerts to the Infrastructure Team when network issues are detected.

### 7.6.3 Clock synchronisation

In order to ensure that accuracy of any logging or monitoring information, the Company's servers and PCs time clocks are synchronised.
All Windows based client PCs synchronise their internal clocks with their server driving the logon procedures.  In turn, all servers periodically synchronise with a master time server on the domain.

### 7.6.3 Data Processing Impact Assessments

A data protection impact assessment (DPIA) is a key requirement under the GDPR and is in essence a risk assessment. Muddy Boots conduct regular DPIA's against our products, logging and mitigating any risks, and maintain a detailed risk register.

## 7.7 Mobile Computing and Working from Home Policy

### 7.7.1 Introduction

This policy applies to all employees using portable and remote working devices including but not limited to: laptops, tablets, mobile phones and USB devices.

### 7.7.2 Staff responsibilities of portable devices

Each staff member has signed a confidentiality clause as part of their contract of employment. This makes clear that all Company information must be treated carefully and must not be disclosed to unauthorised persons.

Within the management of the Company Software assets especially portable devices each staff member will be asked to sign for receipt of the portable device, and to acknowledge that they have read, understood and will comply with this policy.

### 7.7.3 Storing Company data & customer information on mobile devices

Mobile devices have bigger risks of theft or unauthorized access and care must therefore be taken to ensure we do not breach our responsibilities as a trusted software partner and ensure that our own and customers confidentiality is not compromised.

Although we do not encourage Company data & customer information to be stored on mobile devices, there are certain exceptions as long as the following precautions are taken:

- This Policy clearly states that no Company data & customer Identifiable Data are to be stored on any portable machine or device (including a desktop PC) that is not encrypted.
- No Company data & customer identifiable data is to be saved on a non-Company device. The term refers to equipment belonging to any 3rd party as well as personally owned machines.
- Data should only be saved on the Company network, encrypted laptops, tablets & phones.
- All laptops, mobile phones and tablets have a password functionality which enables users to password protect their devices. Users must ensure they activate the password feature, to ensure their devices are password protected (typically this would already be enforced on Company equipment).

### 7.7.4 Physical Security

Laptops and mobile devices are easily lost and are attractive to thieves.

- Portable computers including laptops, PDAs, tablets, etc. must be stored in locked furniture when left unattended.
- Portable devices are never left in plain sight e.g. on the back seat of a car or in a public place
- Staff carrying or using devices off or between company premises must take all reasonable steps to guard against their theft, loss or damage, and against unauthorised use.

- Do not locally store sensitive or confidential information – a contact list or an email message may contain information which is 'sensitive' if it gets into the wrong hands.
- Implement the device's password protection
- Ensure mobile devices are managed through Intune and have remote wipe capability.
- Laptops have full hard disk encryption and remote wipe capability.

In the event that the device is stolen, staff will be expected to report the theft to the police and obtain an incident number. If the device contains data which may come under GDPR, then an ICO breach notification and customer notification will also occur.

Staff members must report the loss or theft of a portable device to their line manager and to the IT Helpdesk immediately. The Infrastructure team can then take appropriate actions to execute remote wipes (if possible), remove the device from the domain, change user's passwords etc. to mitigate security risks.

Negligence in the care of portable devices or failure to report loss or damage at the earliest opportunity may result in disciplinary action being taken against the staff member concerned. All incidents relating to the security of the portable device should be reported using the organisation's incident reporting procedures. This shall include but is not limited to:

- Theft/ loss of portable device
- Disclosure of data to an unauthorised person
- Loss/corruption of data

### 7.7.5 Repairs

Portable devices in need of repair should be logged with the IT helpdesk. A replacement may be issued to the member of staff whilst the repairs are being carried out.

It should be noted that manufacturers' warranties do not normally cover damage caused by misuse or neglect.

### 7.7.6 Passwords/PIN codes/biometrics

Portable devices should adhere to the company password policy previously outlined.

### 7.7.7 Approved usage

Where a portable device is provided by the Company the portable device will be provided to each user pre-loaded with the software approved by the Infrastructure Department.

In case of mobile phones software (apps) for personal use is allowed as long as it does not interfere with company software.

Staff must not make any hardware alterations or additions without approval from the Infrastructure Department.

The Company reserves the right to audit correct usage at any time, and the individual may be held liable for illegally held software or material (e.g. in breach of copyright legislation).

### 7.7.8 Digital imaging and videoing

Photographic recording techniques include photographic film, digital images, video and mobile phones. Any photographs or images are included within the scope of the Data Protection Act 2018 and the GDPR Regulation and attract the same levels of security and confidentiality.

### 7.7.9 Working from home

A company device such as laptop is suitable for working from home and a secure VPN is provided for access to company networks.

All staff are required to use the Company supplied devices and it is not permitted to save any data onto a non-Company machine or device.

### 7.7.10 Staff owned equipment

For prevention of viruses and related security risks staff must not connect any personally owned devices to the Company network, except the Company's wireless network for visitors**.**

Company data of any kind should not be accessed directly on staff owned personal equipment (example a home PC) unless said device is enrolled in the company mobile device management software. These devices will need to be compliant with our Security and IT Policy.

### 7.7.11 Access control from remote locations

The Company systems often need to be accessed from remote locations. This gives rise to extra threats, and, the threat of unauthorised use and unauthorised access to systems and data.

For the purpose of this policy, 'teleworking' is defined as a member of staff whose 'other' authorised space to work is their home location.

The decision as to whether a member of staff will become a 'teleworker' will be made by their line manager, based on the frequency of work being done from home and the equipment required to support it.

For the purposes of teleworking, the Company, at its discretion will provide such staff with a portable laptop. The laptop will remain the property of the Company and must be encrypted by the IT Department.

Any 'Remote worker' will apply all elements of this policy, but in addition will ensure:

- Sensitive information (person identifiable or organisationally sensitive) is locked away when not in use and only accessible by the member of staff.
- Their house and content insurance covers them for the loss of any equipment provided by the employing organisation.

### 7.7.12 Unattended user equipment

Mobile devices are not under any circumstances to be left unattended out of core working hours when working from any Company office.  In the event of a device requiring to be left on premise, it must be locked away by the Infrastructure team.
If a device is seen to be left unattended then it is the responsibility of all employees to notify the Infrastructure team to lock the device away and bring this to the attention of the individual, line manager and HR.

#### 7.7.13 Protection of Data

There are no automatic backup procedures in place for information stored locally on PC or laptop hard disks so staff should use the network drive to store all files.

No personal or sensitive data may be stored on desktop or portable computers unless protected by encryption software as recommended by the Company.

Even with password-protected lock screens and encryption, it is not possible to wholly guard against information on local hard disks being accessed by unauthorised users.

In the event where a computer, or its hard disk, is to be removed from company premises by a Third Party, such as by an engineer when correcting a fault, staff must take care to ensure that any sensitive data is protected.

Removable media should not be used to store sensitive or confidential information. If there is an absolute business requirement to do so this should be only for a short period and appropriate physical and logical security measures should be employed (e.g. data encryption, password controls) and only company supplied storage devices/media should be used. All data should then be securely removed from the media. If removable media containing sensitive or confidential information is lost or stolen this should be reported immediately to the IT Service Desk.

#### 7.7.14 Loaning of Computers

No computer may be removed from company's premises unless authorised and recorded.  Loan computers must be returned by the agreed date and must not be passed on to any other person.

The maximum loan period for computers should be set at two months in order to ensure they are scanned by up to date versions of the anti-virus software.

#### 7.7.15 Virus Scanning

- Staff must allow updates to their anti-virus software when connected to the network, at any time.
- Staff assigned computers that are not regularly attached to the internet must make special arrangements to have anti-virus software regularly updated.

## 8. INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE

### 8.1 Security requirements of systems

Where appropriate, the specification of the new or updated system will include controls regarding the validation of input data, internal processing, and output data, as well as audit trails, activity logs, and user authentication.

This specification process is managed by the Infrastructure manager

### 8.2 Encryption and Cryptographic controls

The Company employs a range of cryptographic controls relevant to the device or application. For example all laptops have fully encrypted hard drives and mobile devices such as tablets and phones are encrypted. Sensitive data that has to be transmitted electronically should also be encrypted.

We will also only use protocols and ciphers for encryption that are deemed to be secure. This is centrally managed by the infrastructure and security teams.

### 8.3 Security in development and support processes

Development, Project and support environments are controlled in order to maintain the security of application system software and information.

- The Company tests all code for security vulnerabilities before release, and regularly scans our network and systems for vulnerabilities
- Network vulnerability assessments
- Selected penetration testing and code review
- Security control framework review and testing
- Desensitized test data

Privacy by design has been embedded into the GDPR for the first time as a legal obligation for both data controllers and processors and states that the data controller shall "implement appropriate technical and organisational measures such as Pseudonymisation which are designed to implement data protection principles such as data minimisation". Muddy Boots development adheres to this approach.

Privacy by default stipulates that the protection of personal data must be a default of all of an organisation's systems and services.

Muddy Boots regularly conduct risk assessments, threat modelling and reviews of our code at both application run-time level and at code level to ensure that where possible, this level of privacy by design is implemented.

#### 8.3.1 Release Control

Live releases are controlled to ensure security of the products. Each product has a security status indicating if release is permitted, this status is updated based on manual and automated security assessment and review of existing security issues in the backlog. All security issues are scored using CVSS3 and these are mapped to internal priority statuses in TFS. Controls are in place to prevent the build up of security issues by enforcing a maximum age on non-critical issues.

Releases would typically be blocked in the following events:

- Discovery of a critical security issue
- A High rated security issue introduced in current sprint
- High rated issues in the backlog older than six sprints
- Medium rated issues in the backlog older than 12 sprints

Release restrictions may be overturned in exceptional circumstances or by agreement with the CTO.

### 8.3.2 Change control procedures

The System Manager is responsible for ensuring that changes to a system do not alter, degrade or compromise:

- Security Controls;
- Access Rights;
- Audit and Security software.

Change management is implemented and the Change advisory board meet regularly to approve requests for change. The controls in place on all software development follow the full System Development cycle from Dev - Test- Staging and then Live. UAT Skim tests and penetration testing is completed to ensure security has not been compromised.

### 8.3.3 Technical review of operating system changes

Operating system changes for non-windows environments hardware are infrequent and are performed by the Infrastructure team.

For Windows systems responsibility for reviewing the implication of operating system changes lies with the Infrastructure department. Scheduled maintenance is carried out each month to ensure all servers are updated. Client devices are set to automatically update and is describe previously in this document that it is the responsibility of the user to ensure they accept the installation of the updates.

### 8.3.5 Covert channels and Trojan code

In order to reduce the risk from covert channels and Trojan code the following guidelines must be adhered to when purchasing software:

- Purchase programs only from a reputable source – refer to Key Supplier list held on the company security area (can be supplied on request)
- In-house written code is written with intetio to follow advised standards and fully tested – refer to Company's WiKi site.
- Use previously evaluated products.
- Control access to code.
- Use staff/contractors of proven trust – refer to key suppliers list on our company Intranet.

### 8.3.6 Outsourced Software Development

Any software development undertaken by outside contractors will be carried out by organisations that are known and proven from prior use or recommendation. Notwithstanding this, the Company tests such systems intensively prior to full deployment. Full NDA's are completed and signed by both parties as well as contracts. We also do not provide any customer or live data for testing and/or development to any third-party organisation.

### 8.3.7 End-User Computing / Software Development

Users should only use the Company approved and supplied systems specifically designed and maintained to hold or process sensitive or personal data. Where users choose to develop and use non-standard systems they are responsible for the security, availability and maintenance of all information contained in that system.

## 9. INFORMATION SECURITY INCIDENT MANAGEMENT

## 9.1 Responding to security incidents and malfunctions

Incidents affecting IT security are reported through the appropriate channels within designated timescales, to minimise the damage and learn from such incidents. GDPR specifies that such timescales are within a 72-hour period for notification of any major incident to both the customer and the ICO.

A security incident is considered to include all actual and attempted breaches in IT security including:

- Viruses.
- Unauthorised access to systems.
- Unauthorised modification of data or systems.
- Unavailability of data or systems because of any of the above points.
- Theft or other loss of equipment of data

Not all of the above would or will warrant a notification to the ICO or customer.

## 9.2 Report security incidents

Staff /Contractors are responsible for the immediate reporting of all security incidents to the IT Service Desk, who will own the security incident and then manage and escalate approximately. Incident reports are created and escalated to the Information Security Group (ISG) and to the ICO if required.

Where there may be inappropriate activity the Infrastructure Manager will inform the user's Line Manager. Customer related security incidents are reported directly to the ISG as per our incident management procedure, again the security incident is raised assessed, actioned, recorded and reported on. Under GDPR Muddy Boots aim to complete this process within a period of 72 hours.

### 9.2.1 Automatic Virus Detection and Reporting

All networked desktop PCs and laptops have Anti-Virus software installed. The software is automatically updated to deal with emerging virus threats.

### 9.2.2 Report to Executive Management

All significant IT security incidents are reported to the ISG.

The information provided is used for statistical purposes and is used to provide feedback. Additionally, it provides a mechanism whereby the effectiveness (or otherwise) of implemented IT Security procedures can be assessed and helps to ensure that counter-measures continue to meet identified threats.

All information is treated in the strictest confidence and any summarised reports, or reports on specific incidents, are anonymised to ensure that the names of the individuals concerned are not disclosed.

### 9.2.4 Reporting software malfunctions

If practical, use of the affected system should be blocked. Users should immediately report the software malfunction to the IT Service Desk.

The symptoms of the problem and any messages appearing on the screen should be noted.

### 9.2.5 Reporting Data Loss

If any device or data media (e.g. USB memory stick) that may contain sensitive information is lost or stolen this must be reported immediately to the IT Service Desk. Any data loss from electronic communication or physical device should also be reported in compliance with our GDPR guidelines published on the Muddy Boots Internet Site at www.en.muddyboots.com, and actioned within the 72-hour timescale as set out under GDPR.

#### 9.2.6 Learning from incidents

The ISG reviews the impact of reported IT incidents, and considers the need for enhanced or additional controls as appropriate. Incident logs and GDPR breach notification logs are maintained on the company Intranet accessible to appropriate staff members in management/infrastructure and security.

#### 9.2.7 Disciplinary Procedures

Managers may, in consultation with HR and the Infrastructure Manager, invoke the Company's disciplinary procedure following an IT security incident. Details of the disciplinary procedure are in the Company Contracts held in the HR System.

## 10. BUSINESS CONTINUITY PLANNING

### 10.1 Introduction

The purpose of business continuity planning is to reduce the disruption cause by disasters and security failures to an acceptable level through a combination of preventative measures and recovery procedures.

The Company considers business continuity planning to comprise two key elements:

- Contingency Planning

  This is undertaken for applications and is the responsibility of System Managers. Contingency plans provide information on how business is performed in the event of unplanned downtime and the procedures for re-establishing the application and the data.

- Disaster Recovery Procedures

  This area is the responsibility of the Head of IT Support and is considered to cover the complete loss of, for example, a computer room or a significant part of the IT Infrastructure.

### 10.2 Disaster recovery procedures

#### 10.2.1 Pre-emptive measures

The Company's backup routines are described in Section 6.4.1. The risk that the data is not recoverable from a backup is considered to be low. Restoration from backup is tested as part of the system implementation process.

#### 10.2.2 Assessment of damage impact and invocation of contingency plans

The Head of IT Support makes an initial assessment of the impact of the disaster and liaises with Technical Director and System Managers as appropriate. System Managers invoke contingency plans where necessary.

The Infrastructure Manager/Head of IT Support, in conjunction with Senior Managers, plans the restoration of systems/applications taking into account interdependencies between business processes.

### 10.2.3 Restoration of physical location

The Company have a full DR site for the live environment based at their Headquarters in Phocle Green, Ross-On-Wye, Hereford.

### 10.2.4 Electrical, network, cabling and leased lines

The co-operation of the Infrastructure Team is critical to the restoration of the network infrastructure.

The Company have a contracted electrician to provide support for the UK offices.

The main datacentre electrical support is under contract with 6DG.

The construction or re-construction of the local LAN infrastructure will be undertaken in conjunction with the Company's Infrastructure Department.

### 10.2.5 Hardware replacement – Data Communications equipment

The Infrastructure Team will provide details of data communications equipment required.  This equipment is purchased through preferred suppliers where accounts are already in place. The providers can also supply, install and configure the equipment if required.

### 10.2.6 Hardware replacement – Servers

The replacement of server hardware, required for all other systems, will be sourced by Infrastructure staff.

### 10.2.7 Re-installing applications and restoring backups

The Infrastructure Department are responsible for the reinstallation of application software and the restoration of backup data as outlined in contingency plans.

### 10.2.8 PCs and peripherals

Infrastructure staff will be responsible for the relocation of equipment to temporary accommodation and/or for the procurement of replacement equipment.

### 10.2.9 Denial of Service Mitigation

Infrastructure staff will be responsible for remediation and process for restoration of systems in the event of a denial of service attack.

DDoS attacks often take the form of flooding the network with unwanted traffic; some attacks focus on overwhelming resources of a specific system. Create a whitelist of the source IPs and protocols you must allow if prioritizing traffic during an attack. Include your big customers, critical partners, etc.

In the event of a DOS attack, infrastructure will contact our hosting services to inform them that we will instigate renewal of URL/IP entry points , and inform customers accordingly.

## 11. COMPLIANCE WITH LEGAL REQUIREMENTS

Information systems must be operated and managed in a way that avoids breach of any criminal and civil law, statutory, regulatory or contractual obligations and of any security requirements.

### 11.1 Identification of applicable legislation

These are implemented through a range of regional and local policies and procedures. Legislation includes but is not limited to:-

- The Data Protection Act 2018
- The General Data Protection Regulation
- The Copyright, Designs and Patents Act 1988
- The Computer Misuse Act 1990
- The Health and Safety at Work Order (1978) and Health and Safety (Display Screen Equipment) Regs 1992
- The Human Rights Act (1998)
- The Employment Practices Data Protection Code
- The Telecommunications (Lawful Business Practice) Regulations 2000
- PECR – privacy and electronic communication Regulations
- The Waste Electric and Electronic Equipment (WEEE) Regulations 2013

Additionally, staff are under a contractual obligation to preserve the confidentiality of this information.

The Company will show compliance by the internal and external audits performed in line with ISO27001. We have also attained HMG Cyber essentials certification (Jan 2018 updated on an annual basis).

### 11.2 Software copyright

All software on IT equipment must be legitimate, and licensed to the Company. In most instances the copying of software is illegal, although the law does recognise the need for legitimate backup copies to be made.

Only software authorised by the Infrastructure Department must be installed on PCs. Auditing software enables IT staff to remotely monitor unauthorised changes in PC hardware or software configurations.

The use or installation of any software other than that authorised by the Infrastructure Department may lead to disciplinary action.

The Service Catalogue and IT Asset register includes details of software licences and their installed locations.

## 11.3 PCI Compliance Policy

### 11.3.1 Policy Statement

PCI DSS (Payment Card Industry Data Security Standard) is a requirement if a merchant agrees to accept credit cards as a form of payment and is intended to help merchants protect their customers from fraudulent transactions.

Annually, merchants will be required to complete a Self-Assessment form issued through the PCI Security Standards Council regarding their policies and procedures related to credit card processing. To be compliant, merchants will need to sign this statement and answer each question to the best of their ability. By strictly limiting what the company does with credit cards, our scope of compliance becomes very limited.

In addition, the company agrees to be scanned by an independent third-party scanning provider. The third party will attempt to penetrate the company's systems. Should it succeed, it will report to us any vulnerability and the source of the vulnerability that the company will need to fix to stay within PCI compliance.

This policy shall be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment.

### 11.3.2 Adherence to Standard

The company have been assigned SAQ B 3.1 level of standards to adhere to, to be PCI compliant, by a third-party company assigned by the company's bank based on the following criteria:

- Only a point of sale terminal and/or an imprint machine that does not use a data line is used
- Any card holder data that we keep is in paper form (like receipts or copy of receipts)
- We do not store cardholder data electronically.

### 11.3.3 Handling of Cardholder data

- Cardholder data must be deleted after processing in a way that makes the data unrecoverable.
- All media must be destroyed when it is no longer needed for business or legal reasons. Acceptable methods to destroy paper media include cross-cut shredding, burning and/or pulping to make sure that the data cannot be reconstructed  Information from the magnetic stripe must not be stored.
- The primary account number or PAN (usually 16 digits; the main number on the front of the card) needs to be masked whenever displayed or printed. Masking entails not displaying or replacing all numbers with a pad character (such as an *) with the last four digits being the only visible numbers from the PAN. The full number may be displayed on the merchant copy if necessary, but never on the customer copy of receipts.
- The card verification code (the three or four-digit number from the back of the card) cannot be stored.
- Unencrypted Primary Account Numbers may not be sent via email may not be sent via email, text, chat or any unencrypted method.

### 11.3.4 Access to cardholder data

Access to system components and cardholder data is limited to only those individuals whose jobs require such access, as follows:

- Restriction of access to privileged user to least privileges necessary to perform job responsibilities,
- Assignment of access based on individual personnel's job classification and function
- Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved.

11.3.5 Personnel training and awareness

- Regular security testing and training of staff by the Security Team.
- Challenge culture within offices
- Not installing or replacing devices without verification
- Reporting suspicious behaviour or device tampering to the correct personnel within the Infrastructure department.

.

### 11.4 Intellectual Property Rights

Please refer to the Company Contract in HR System and the Company Policies and Procedures area in the Company Intranet

### 11.5 Data protection and privacy of personal information

Please refer to the Company Contract in HR System and the Company Policies and Procedures area in the Company Intranet. Please also refer to our privacy and GDPR policies published online at https://en.muddyboots.com/policies

### 11.6 Prevention of misuse of information assets

All use of the Company Offices and equipment must be for legitimate business purposes, and their use by employees for non-business or unauthorised purposes is regarded as improper use. If such improper activity is identified, the employee's manager must take the appropriate disciplinary action.

### 11.7 Compliance with Security Policy

The ISG are responsible for the review of this Security and IT Policy. Compliance with the policy rests with a range of staff, as described throughout this document. Ultimate responsibility rests with the Chief Executive.

### 11.8 Technical compliance checking

Tests to ensure that Information System comply with controls are carried out during implementation or system upgrades, under the technical guidance and supervision of the appropriate manager.

## 12. INFORMATION SECURITY IN SUPPLIER RELATIONSHIPS

All supplier relationships involving information assets are within the scope of this policy; these include:

- Service providers.
- Managed security services.

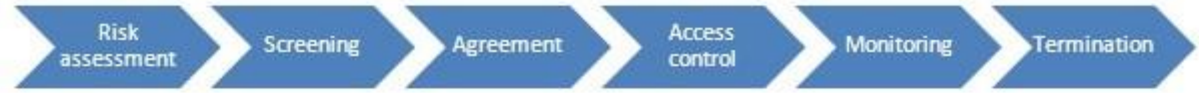
- Customers.
- Outsourcing suppliers (facilities, operations, IT systems, data collection, call centres, others).
- Consultants and auditors.
- Developers and suppliers of IT systems and services.
- Cleaning, catering and other outsourced support services.
- Temporary personnel, placement and other (casual) short-term appointments.

### 12.1 Responsibilities

The Infrastructure Manager at Muddy Boots Software is responsible for ensuring that information security is addressed in all supplier relationships before agreements are signed and any access granted; responsible for the risk assessment where required.

### 12.2 Process

Muddy Boots Software Limited's policy for supplier relationships follows the process:



**Risk assessment** Assess the risks to confidentiality, integrity and availability of information outsourced as part of our processes or allowing a third party to access our information. The next steps are dependent on the results of risk assessment - for example, we may not need to perform a background check or insert security clauses for a cafeteria supplier, but will need to do it for a software developer.

**Screening / auditing.** Background checks completed on potential suppliers or partners – the more risks that were identified in the previous step, the more thorough the check needs to be; always staying within the legal limits.

**Selecting clauses in the agreement.** Once the risks have been identified the security clauses will be drafted, which need to be inserted in an agreement. There may be dozens of such clauses, ranging from access control and labelling confidential information, all the way to which awareness trainings are needed and which methods of encryption are to be used.

**Access control.** Although an agreement is in place access is still set based on a "Need-to-know basis."

**Compliance monitoring.** Monitor and, if necessary, audit whether they comply with all the clauses.

**Termination of the agreement.** No matter whether the agreement has ended under friendly or less-than-friendly circumstances, all assets must be returned and all access rights removed.