Wise Digital Media (Staffwise)
Access Control Policy

1. Introduction

This document sets out the measures to be taken by all employees of Wise Digital Media (Staffwise) (the “Company”), by authorised third parties, and by the Company as a whole with respect to the control of access (both electronic and physical) to the Company’s IT Systems.

2. Definitions

“Admin Password” means a password for any IT Systems that are not for normal use by Users including, but not limited to, servers and networking equipment;

“Data Protection Officer” means the Company’s data protection officer, Gemma Lennard, 07707647262;

“IT Department” means the IT Manager and the IT Staff responsible for the administration, installation, and maintenance of the IT Systems, contact details can be found within the Business Continuity Plan;

“IT Manager” means the manager of the IT Department, Mark Waddington, 07702050206;

“IT Security Breach” means any incident involving the unauthorised access to any IT Systems or to the data stored on the IT Systems

“IT Staff” means all staff working under the authority and supervision of the IT Manager in the IT Department;

“IT Systems” means desktop and laptop computers, mobile devices, servers, networking equipment and other infrastructure, computing environment, and any and all other relevant equipment;

“Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed;

“User” means all employees and agents of the Company and any and all third parties authorised to use the IT Systems including, but not limited to, contractors and sub-contractors;

“User Account” means the login details and account assigned to a User for access to and use of the IT

Systems in accordance with this Policy; and

"User Password" means the password for a User Account.

3. Scope and Key Principles

3.1 This Policy applies to all employees of the Company and any and all third parties authorised to use the IT Systems including, but not limited to, contractors and sub-contractors (collectively, "Users"). All Users must ensure that they are familiar with this Policy and must adhere to and comply with it at all times.

3.2 All Users must use the IT Systems only within the bounds of UK law and must not use the IT Systems for any purpose or activity which is likely to contravene any UK law whether now or in the future in force.

3.3 All Users must use the IT Systems in accordance with this Policy and all related Company Policies including, but not limited to, the IT Security Policy; Data Protection Policy; Confidential Information Policy; Anti-Malware Policy; Communications, Email, Internet & Social Media Policy; and (where applicable) Bring Your Own Device (BYOD) Policy.

3.4 All IT Systems are to be protected against unauthorised access.

3.5 All line managers must ensure that all Users under their control and direction adhere to and comply with this Policy at all times as required under Paragraph 3.1.

3.6 This Policy outlines how User Accounts and access privileges are to be created, managed, and removed, as required. User Accounts and access privileges shall be determined and granted in accordance with this Policy and shall be reviewed and, if necessary, revoked as set out herein.

3.7 Access privileges for all IT Systems (electronic and physical) shall be determined on the basis of business need and the principle of "least privilege". Users shall be provided only with the minimum levels of access to IT Systems that are needed to perform their job role effectively.

3.8 This Policy also sets out controls designed to prevent Users from obtaining unauthorised access or privileges.

3.9 All data stored on IT Systems shall be available only to those Users with a legitimate need for access.

3.10 All data stored on IT Systems shall be protected against unauthorised access and/or processing.

3.11 All Users must report any and all security concerns (including, but not limited to, IT Security Breaches) relating to the IT Systems or to the data stored thereon immediately to the IT Department. If any such concerns relate in any way to personal data, such concerns must also be reported to the Data Protection Officer.

4. Electronic Access Control

4.1 As stated above in paragraph 3.7, access privileges for all IT Systems shall be determined on the basis of Users' levels of authority within the Company and the requirements of their job roles in accordance with the principle of "least privilege". Users shall not be granted access to any IT Systems or electronic data which are not reasonably required for the fulfilment of their job roles.

4.2 The IT Department shall implement User Account management procedures for the registration, modification, and revocation (temporary and permanent) of User Accounts on all IT Systems.

4.3 Where any User Account is not used for a period of 30 days, unless previously agreed in writing between the User concerned and the IT Department, that User Account shall be made inactive for a period of 30 days prior to deletion unless reactivation or other authorised access is required.

4.4 Where any User's job role or the requirements of that job role change, the access privileges applicable to that User's User Account shall be reviewed and modified where necessary.

4.5 Where any User ceases to have a relationship with the Company, whether as an employee or in their capacity as a third party (including, but not limited to, a contractor or sub-contractor), that User's User Account shall be made inactive for a period of 30 days prior to deletion unless further authorised access is required.

4.6 All User Accounts (including inactive and/or redundant User Accounts) shall be reviewed on a 6 month basis by the IT Department in order to determine:

a) whether access privileges for each User are appropriate or should be modified;

b) whether any User Account should be suspended;

c) whether any suspended User Account should be re-activated;

d) whether any suspended, inactive, and/or redundant User Accounts should be deleted;

4.7 Where any User Account is created, modified, suspended, re-activated, or identified as inactive and/or redundant, the action should be logged in using the 'User Account Request/Change Request Form.'

5. Password and Device Security

5.1 All IT Systems (and in particular mobile devices including, but not limited to, laptops, tablets, and smartphones) shall be protected with a secure password or passcode, or such other form of secure log-in system as the IT Department may deem appropriate and approve. Users should note that not all forms of biometric log-in are considered secure. Only those methods approved by the IT Department may be used.

5.2 Where any new hardware or software has a default password when it is purchased by and/or supplied to the Company, the default password must be changed in accordance with the requirements of this Part 5 before the hardware or software is put into active use on any live system.

5.3 All User Passwords must, where the software, computer, or device allows:

a) be at least 12 characters long;

b) contain a combination of upper and lower case letters, numbers and symbols;

c) be changed at least every 30 days (password changes shall be software-enforced where possible);

d) be different from any previous password;

e) not be obvious or easily guessed (e.g., birthdays or other memorable dates, memorable names, events, or places etc.); and

f) be created by individual Users.

5.4 All Admin Passwords for IT Systems must, where the software, computer, or device allows:

a) be at least 12 characters long;

b) contain a combination of upper and lower case letters, numbers and symbols;

c) be changed at least every 30 days (password changes shall be software-enforced where possible);

d) be different from any previous password;

e) not be obvious or easily guessed (e.g., birthdays or other memorable dates, memorable names, events, or places etc.); and

f) be created by the IT Department.

5.5 User Passwords should be kept secret. Under no circumstances should a User share their User Password with anyone, including the IT Department. No User will be legitimately asked for their User Password by anyone at any time and any such request should be refused. If a User has reason to believe that another individual has obtained their User Password, they should change it immediately and report it to the IT Department as a suspected IT Security Breach and, where personal data could be accessed by an unauthorised individual, to the Data Protection Officer.

5.6 Admin Passwords should be kept confidential within the IT Department or to specific authorised IT Staff if not all IT Staff are authorised to use a particular Admin Password. If there is reason to believe that any such Admin Password has been obtained by anyone who is not authorised to use it, this must be reported to the IT Manager as a suspected IT Security Breach, whereupon, the IT Manager shall change the affected Admin Password or instruct that it is changed. Where personal data could be accessed by an unauthorised individual, the suspected IT Security Breach must also be reported to the Data Protection Officer.

5.7 If a User forgets their User Password, they may reset it by using the forgot password link. Alternatively, the forgotten User Password should be reported to the IT Department. The IT Department will take the necessary steps to restore the User's access to the IT Systems which may include the issuing of a temporary User Password, which may be fully or partially known to the member of the IT Staff responsible for resolving the issue. A new User Password must be set up by the User immediately upon the restoration of access to the IT Systems.

5.8 Passwords should not be written down if it is possible to remember them. If a password is not easy to remember, it should be stored securely (e.g., in a locked drawer or in a secure (IT Department-approved) password app or database) and under no circumstances should passwords be left on display for others to see (e.g., by attaching a note to a computer display).

5.9 All IT Systems with displays and user input devices (e.g., mouse, keyboard, touchscreen, etc.) shall be protected, where possible, with a password protected screensaver or sleep/standby mode that will activate after 2 minutes of inactivity. This time period cannot be changed by Users and Users may not disable the screensaver or sleep/standby mode. Activation of the screensaver or sleep/standby mode will not interrupt or disrupt any other activities taking place on the computer (e.g., a User's work).

5.10 All mobile devices (including, but not limited to, laptops, tablets, and smartphones) provided by the Company shall be set to lock, sleep, or similar, after 2 minutes of inactivity, requiring a password, passcode, or other form of log-in to unlock, wake, or similar. This time period cannot be changed by Users and Users may not disable the auto lock, sleep, etc. Activation of such a mode will not interrupt or disrupt any other activities taking place on the device (e.g., a User's work).

5.11 Users may not use any software which may allow outside parties to access the IT Systems without the express consent of the IT Manager. Any such software must be reasonably required by the User for the performance of their job role and must be fully inspected and cleared, and logged in writing using the User Account Request/Change Request Form by the IT Manager. Where such access renders personal data accessible by the outside party, the Data Protection Officer must also fully inspect and clear the software and log the same in writing using the 'User Account Request/Change Request Form.'

5.12 Users may connect their own devices (including, but not limited to, laptops, tablets, and smartphones) to the Company networks subject to the approval of the IT Department. Any and all instructions and requirements provided by the IT Department governing the use of Users' own devices when connected to the Company network must be followed at all times. Users' use of their own devices shall be subject to, and governed by, all relevant Company Policies (including, but not limited to, this Policy) while those devices are connected to the Company network or to any other part of the IT Systems. The IT Department shall reserve the right to request the immediate disconnection of any such devices without notice.

6. Physical Access Control

6.1 Wherever practical, IT Systems will be located in rooms which may be securely locked when not in use or, in appropriate cases, at all times whether in use or not (with authorised members of the IT Department and any other authorised Users being granted access by means of a key, smart card, door code or similar). Where access to such locations is restricted, no unauthorised access to such locations shall be permitted for any reason.

6.2 All IT Systems not intended for normal use by Users who are not members of the IT Department (including, but not limited to, servers, networking equipment, and network infrastructure) shall be located, wherever possible and practical, in secured, climate-controlled (where appropriate or necessary) rooms and/or in locked cabinets which may be accessed only by authorised members of the IT Department.

6.3 No Users that are not members of the IT Department shall have access to any IT Systems not intended for normal use by Users (including such devices mentioned above in Paragraph 6.2) without the express permission of the IT Manager. Under normal circumstances, whenever a problem with such IT Systems is identified by a User, that problem must be reported to the IT Department. Under no circumstances should a User attempt to rectify any such problems without the express permission (and, in most cases, instruction and/or supervision) of the IT Manager.

6.4 In the event that a key or smart card required for access to any IT Systems is lost, the loss must be immediately reported to the IT Manager. If the room or cabinet in question has a key-operated lock, the lock shall be changed, and new keys issued to all authorised personnel. If the lock is operated by smart card or similar, the lost card (etc.) shall be cancelled and a replacement issued.

6.5 Where any locks are operated via door code, codes should be kept secret. Under no circumstances should a code be shared with any unauthorised personnel. If there is reason to believe that an unauthorised individual has obtained a door code, this must be reported as a suspected IT Security Breach to the IT Manager. In the event that the affected door code is changed, all authorised personnel shall be informed of the new code.

6.6 Wise Digital Media (Staffwise) will conduct a quarterly review of users with physical access to the office space.

6.7 Access Restriction Control;

Locks: All entry points and restricted areas shall be equipped with appropriate locking mechanisms. Locks shall be regularly inspected and maintained to ensure functionality.

Visitor Logs**:** A comprehensive visitor logging system shall be maintained at all entry points. Visitors must register their details including name, purpose of visit, time of arrival, and departure. Visitor logs are retained and maintained for a minimum period of 6 months.

Third parties: Contractors and subcontractors will be issued with a photo ID badge after company personnel check ID badges and complete the visitor log before gaining access to the premises. Unauthorized entry is strictly prohibited.

Video Surveillance: a. Video surveillance cameras shall be strategically installed throughout the premises to monitor key areas. b. Surveillance footage shall be continuously recorded and stored securely for a period of 6 months. c. Regular checks and maintenance of surveillance equipment shall be conducted to ensure optimal performance.

Compliance: a. All employees shall be briefed on the physical access control procedures and their responsibilities. b. Compliance with access control measures is mandatory for all personnel. c. Violations of access control policies shall be subject to disciplinary action.

7. Reporting IT Security Breaches

7.1 Subject to Paragraphs 7.2 and 7.3 and any other provision in this Policy to the contrary, all concerns, questions, suspected IT Security Breaches, or known IT Security Breaches shall be referred immediately to the IT Department**.**

7.2 All concerns, questions, suspected IT Security Breaches, or known IT Security Breaches that involve personal data (i.e., where a Personal Data Breach is or may also be involved) shall be referred immediately to the Data Protection Officer, who shall handle the matter in accordance with the Company’s Data Protection Policy.

7.3 All concerns, questions, suspected IT Security Breaches, or known IT Security Breaches that involve confidential information shall be referred immediately to the IT Department, who shall handle the matter in accordance with the

Company's Confidential Information Policy.

7.4 Upon receiving a question or notification of an IT Security Breach, the IT Department shall, within 24 hours, assess the issue including, but not limited to, the level of risk associated therewith, and shall take any and all such steps as the IT Department deems necessary to respond.

7.5 Under no circumstances should a User attempt to resolve an IT Security Breach on their own without first consulting the IT Department or the Data Protection Officer, as appropriate. Users may only attempt to resolve IT Security Breaches under the instruction of, and with the express permission of, the IT Department.

7.6 All IT Security Breaches, whether remedied by the IT Department or by a User under the IT Department's direction, shall be fully documented in the Data Breach Report Form.

8. Policy Review

The Company shall review this Policy not less than annually and otherwise as required in order to ensure that it remains up-to-date and fit for purpose. All questions, concerns, and other feedback relating to this Policy should be communicated to the IT Manager, Mark Waddington or the Data Protection Officer, Gemma Lennard.

9. Implementation of Policy

This Policy shall be deemed effective as of 01.01.2022. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Name:	Gemma Lennard
Position:	Data Protection Officer
Date:	08th January 2025
Due for Review by:	08th January 2026
Signature:	GL