Title:	**User and Password Management Policy**
Version:	**1.1**
Date:	**March 2018**
Reviewed:	**March 2018**
To be reviewed:	**December 2020**
Classification:	**Public**

1. Introduction

This Access Management Policy is a sub-policy of the Information Security Policy and sets out the requirements for the effective management of user accounts and access rights. This management is essential in order to ensure that access to DMT-hosted information and information systems is restricted to authorised users.

2. Scope

All information systems used to conduct DMT business must be managed in accordance with this policy.

This Policy applies to all DMT employees, Trustees, Committee members, temporary staff, contractors and third parties who have access to information systems or information held in any form whether digital or physical (hardcopy) by DMT on behalf of itself, or its stakeholders.

3. Eligibility

User accounts for relevant business critical systems will only be provided for:

- Current DMT staff
- Those who are granted associate status. (Associates will include staff from other organisations which provide services to the DMT who may require access to the DMT's information systems in order to fulfil their contractual obligations to the DMT). The DMT may also provide access to a limited range of services to former staff (typically restricted to allowing them to manage transfer of email to a new account).

Authorisation to manage

The management of user accounts and privileges on the DMT's information systems is restricted to suitably trained and authorised members of staff.

Account and privilege management

Accounts will only be issued to those who are eligible for an account and whose identity has been verified.

On issue of account credentials, users must be informed of the requirement to comply with the DMT's Information Security policy.

Access rights granted to users will be restricted to the minimum required in order for them to fulfil their roles. Procedures shall be established for all information systems to ensure that users' access rights are adjusted appropriately and in a timely manner to reflect any changes in a user's circumstances (e.g. when a member of staff changes their role or a leaves the DMT).

4. Legislation

DMT is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to Employees and agents of DMT, who may be held personally accountable for any breaches of information security for which they may be held responsible. DMT shall comply with the legislation as stated in the Applicable Legislation Notice as a minimum and shall also abide by any regulatory requirements or business/contractual obligations at all times.

5. General Access Control

No user of DMT network may release or permit the release of any data maintained in the computer files to any person or persons without express written approval of the Information Asset Owner ('IAO') or their delegated authority. DMT operate an asset Data Classification Policy and all access will be mindful of the possible risks and impacts, relative to the classifications of the assets, which become accessible to the user as a consequence of the proposed access. The DMT IT Systems, due to their size, have specific areas with restricted access due to the Classification of the assets stored in them rather than completely segregated systems by classification;

- Any agency or third party responsible for the collection and maintenance of such data must not release or permit access to the data, except for legal requirements as solely requested in the performance of audits, and as prescribed by law;

- All controls for physical and logical access must be allocated to Users on a "requirement for access" and "need to know" basis;

- All incoming and outgoing mail points, facsimile machines, photocopiers and scanning devices should be appropriately positioned and available for only authorised Employees

- Any third party access to the DMT information assets, including the corporate network, must be with the approval of the IT Manager.

- All Users must be registered in accordance with DMT user registration procedure, where users must be granted access rights appropriate to their role and function only;

- Users should in so far as is reasonably possible and if it supports business requirements be granted access to data information or resources on the basis of the 'principle of least privilege' and if a resource or a function is not required for their specific work tasks, then it should not be granted to the user;

- There must be regular documented reviews of User access rights – including third parties and temporary Users – to ensure all Users' access is appropriate to their needs and redundant access is promptly removed;

- Should any User change role and/or function, all access rights must be modified to reflect that change;

- Should Users be granted temporary leave for sickness, maternity, compassionate or

associated leave, their accounts must be disabled until they return to active duty;

- It is advised that where possible job roles and functions, including system administrators, have appropriate access controls pre-defined for consistency and ease of allocation upon User registration.

6. User Access Management

- Every User of DMT network must have an individual network account;
- Each network account must have a unique identifier and must have the User identified;
- Network Users with multiple roles may be required to have a unique network account for each distinct role;
- Each network account shall be set to disable access to the network after 3 failed logon attempts until reset/unlocked by the IT Manager or his delegated representative;
- User accounts shall be reviewed annually and changes of status or role of any employee shall be advised to the System Administrator by HR and all Line Managers; and
- Standard network User accounts or any information related to them must not be shared between employees.

7. New network accounts

- DMT exercises a formal documented and auditable User registration and deregistration process for all network Users, permanent and temporary;
- All requests to the System Administrator for new accounts are to be made by the Executive Director prior to the employee starting work, with all required access specified;
- All new User account holders will receive a copy of the Acceptable Use Policy. During employment, changes to roles/rights will similarly be documented and presented for signature by the User acknowledging the scope of access rights;
- New accounts are created with a randomly generated password which the User must not divulge to any other person and be changed on the Users first logon to a new one known only to them; and
- Passwords must only be given in person to the new employee after verification of their identity.

8. Account Removal

- If an Employee or other authorised user leaves DMT, all network accounts for that person shall be disabled immediately. A deletion date shall be entered into the account of 60 days from the date of disablement;
- Information assets of the User leaving (Email account folders and file folders specific to one user/role) will be examined by a line manager for appropriate sanitisation and/or reallocation of access rights to another User, where continuing access is required;
- All network accounts that reach their deletion date shall be deleted; and
- Accounts used by an Employee on long-term absence shall be disabled, unless specifically requested by the line manager.

9. Administrator Accounts

- Administrator and 'Privileged User' (defined as a user of a personal computer who has the ability to use advanced features of programs which are beyond the abilities of "normal" users, but is not necessarily capable of programming and system administration) accounts must be authorised by the System Administrator;
- All activities of administrator accounts shall have audit logs enabled, giving a full audit trail of actions; and
- Standard User accounts shall not have network or local computer administrative rights/access.

10. Administrator Network and System Access

- Responsibilities should be allocated and segregated to reduce opportunities for unauthorised or unintentional modification or misuse. User administration rights for all systems, IT devices, networks and network services, including segregation of duties (whether administration segregation, domain segregation or VLAN segregation etc.), should be formally recorded and reviewed for auditing and accountability purposes;
- Groups of services, Users and systems should also be segregated on DMT networks;
- Access controls shall take into account shared networks (e.g. between DMT business departments) and access to these networks shall be in line with this Policy;
- To ensure that network connections and information flows do not breach this Policy, appropriate routing controls shall be applied;
- All means of access to the networks and their services should be formally documented within network procedural documentation, regularly reviewed and updated upon change;
- Access to network services is only permitted on a 'need to know' basis by nominated Users within DMT's IT services provider, as defined by their job role;
- The System Administrator of the network may revoke access rights to the network should there be a reason to suspect malicious intent, compromising confidentiality, integrity and availability of DMT data;
- All network and System Administrators must be appropriately trained;
- Network and System Administrators must ensure that administrative functions are not made available to normal Users;
- Automatic equipment identification should authenticate connections;
- Changes to all physical and logical access to diagnostic and configuration ports should be controlled and formally documented within network procedures and monitored on a regular basis;
- Access to all system utilities and tools must be restricted, and only made available to a limited number of privileged authorised Users. All activities should be formally logged. Any utilities not used or not core to business requirements should be disabled or removed; and
- System application and network sessions should 'time-out' after a defined period of inactivity and limitations on connection times should be considered for high risk applications.

11. Account Authentication

All user accounts shall be authenticated using passwords as a minimum. Further information can be found in the Password Management section below.

Single sign-on

- DMT uses a single-sign on to the network server and locally hosted applications such as email, spam filter etc.
- Remote login to the DMT systems also use the single sign-on.

Externally hosted applications

- Remotely hosted applications must not use the network password; and
- Passwords for such applications must follow the same guidelines as provided in the DMT Password Policy.

Scheduled Account Review

- All network accounts shall be reviewed on a 3-monthly basis;
- Accounts that have not been used for 3 months shall be automatically disabled; and
- Unused accounts that have been disabled for a month or longer shall be deleted on verification with the account holders Line Manager.

Responsibilities

- The Executive Director has ultimate responsibility for compliance with this Policy.
- DMT Employees and if applicable Contractors or Third Parties are responsible for adherence to this Policy and its associated procedures.

12. Training

As part of DMT ongoing commitment to implementing and further developing this Policy, DMT is committed to regularly educating, training and raising awareness of employees on the Policy and of any further commitments required by DMT to conform to any relevant legislation.

13. Monitoring

This Policy shall be monitored and subject to regular review which shall take place annually, or when a significant change is made to the systems, people or processes related to this Policy.

14. Non Compliance

There is a requirement for all Employees to comply with this Policy, and where requested, to demonstrate such compliance. Failure to comply with the Policy shall be regarded as a disciplinary offence, and shall be dealt with under the Disciplinary Process.

15. Password management

All system-level passwords (e.g., root, enable, Windows Administrator, application administration accounts, etc.) must be changed on at least a quarterly basis, or more frequently for more sensitive system accounts.

All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 45 days.

Weak Passwords are not permitted on any DMT systems user or administrator accounts. All users at DMT should be aware of how to select strong passwords.

Strong passwords must contain at least three of the five following characteristics:

- Lower case characters
- Upper case characters
- Numbers
- Punctuation
- “Special” characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc.)

DMT password quality policy, which shall be automatically enforced within systems, where possible, is as follows:

- Passwords shall be kept confidential;
- Passwords shall not be shared;
- Passwords shall conform to the entropy for Strong Passwords detailed above;
- Passwords shall not be stored on paper, software file or hand held device;
- If you think a password has been compromised change it immediately;
- When changing your password, staff shall not use one that you have used recently for that account;
- Passwords shall have a minimum of 8 characters, and shall contain at least one non-alphanumeric character;
- Passwords shall not be the same as your user id or name, and shall not be easily guessed by someone who knows you well;
- Passwords used for business purposes shall not be the same as used for non-business purposes;
- Temporary passwords shall be changed at first login;
- Passwords shall not be included in any automated logon process.

If an account or password compromise is suspected, it should be reported to the System Administrator immediately.