Access Control Policy

Version: 1.0
Date: 24th May 2018
Author: MRC Print Limited

Passwords

Choosing Passwords

Passwords are the first line of defence for our systems and together with the user ID help to establish that people are who they claim to be.

A poorly chosen or misused password is a security risk and may impact upon the confidentiality, integrity or availability of our computers and systems.

Weak and strong passwords

A weak password is one which is easily discovered, or detected, by people who are not supposed to know it. Examples of weak passwords include words picked out of a dictionary, names of children and pets, car registration numbers and simple patterns of letters from a computer keyboard.

A strong password is a password that is designed in such a way that it is unlikely to be detected by people who are not supposed to know it, and difficult to work out even with the help of a computer.

Everyone must use strong passwords with a minimum standard of:

- At least eight characters
- Contain a mixture of alpha and numeric digits, with at least one digit
- More complex than a single word (such passwords are easier for hackers to crack)

The Government advises using Environ passwords with the following format: consonant, vowel, consonant, consonant, vowel, consonant, number then number. An example for illustration purposes is provided below:

- pinray45
- dogham80

Protecting Passwords

It is of utmost importance that the password remains protected at all times. The following guidelines must be adhered to at all times:

- Never reveal your passwords to anyone
- Never use the 'remember password' function
- Never write your passwords down or store them where they are open to theft
- Never store your passwords in a computer system without encryption

- Do not use any part of your username within the password
- Do not use the same password to access different MRC Print Limited systems
- Do not use the same password for systems inside and outside of work

Changing Passwords

All user-level passwords must be changed at a maximum of every 180 days, or whenever a system prompts you to change it. Default passwords must also be changed immediately. If you become aware, or suspect, that your password has become known to someone else, you must change it immediately and report your concern to the appropriate person.

Users must **not** reuse the same password within XX password changes.

System Administration Standards

The password administration process for individual MRC Print Limited systems is well documented and available to designated individuals.

All MRC Print Limited IT systems will be configured to enforce the following:

- Authentication of individual users, not groups of users - i.e. no generic accounts
- Protection with regards to the retrieval of passwords and security details
- System access monitoring and logging - at a user level
- Role management so that functions can be performed without sharing passwords
- Password admin processes must be properly controlled, secure and auditable

Employee Access

User Access Management

Formal user access control procedures must be documented, implemented and kept up to date for each application and information system to ensure authorised user access and to prevent unauthorised access. They must cover all stages of the lifecycle of user access, from the initial registration of new users to the final deregistration of users who no longer require access. These must be agreed by MRC Print Limited. Each user must be allocated access rights and permissions to computer systems and data that:

- Are commensurate with the tasks they are expected to perform
- Have a unique login that is not shared with or disclosed to any other user
- Have an associated unique password that is requested at each new login

User access rights must be reviewed at regular intervals to ensure that the appropriate rights are still allocated. System administration accounts must only be provided to users that are required to perform system administration tasks.

User Registration

A request for access to MRC Print Limited computer systems must first be submitted to the appropriate department for approval. Applications for access must only be submitted if approval has been gained from the appropriate person.

When an employee leaves MRC Print Limited, their access to computer systems and data must be suspended at the close of business on the employee's last working day. It is the responsibility of the appropriate person to request the suspension of the access rights via the designated department – e.g. Information Services Helpdesk.

User Responsibilities

It is a user's responsibility to prevent their user ID and password being used to gain unauthorised access to MRC Print Limited systems by:

- Following the Password Policy Statements outlined as above
- Ensuring that any PC they are using that is left unattended is locked or logged out
- Leaving nothing on display that may contain access information such as login names and passwords
- Informing the appropriate person of any changes to their role and access requirements

Network Access Control

The use of modems on non MRC Print Limited owned PC's connected to MRC Print Limited network can seriously compromise the security of the network. The normal operation of the network must not be interfered with. Specific approval must be obtained from the appropriate department before connecting any equipment to the MRC Print Limited network.

User Authentication for External Connections

Where remote access to the MRC Print Limited network is required, an application must be made via the appropriate person. Remote access to the network must be secured by two-factor authentication consisting of a user name and one other component, for example a password.

Supplier Remote Access to The MRC Print Limited Network

Partner agencies or third party suppliers must not be given details of how to access the MRC Print Limited network without permission from the appropriate person. Any changes to supplier's connections must be immediately sent to the appropriate person so that access can be updated or ceased. All permission and access methods must be controlled by the appropriate person.

Partners or third party suppliers must contact the appropriate person before connecting to the MRC Print Limited network and a log of activity must be maintained. Remote access software must be disabled when not in use.

Operating System Access Control

Any access to operating systems is controlled by a secure login process. The access control defined in the User Access Management section and the Password section above must be applied. The login procedure must also be protected by:

- Not displaying any previous login information e.g. username
- Limiting the number of unsuccessful attempts and locking the account if exceeded
- The password characters being hidden by symbols
- Displaying a general warning notice that only authorised users are allowed

All access to operating systems is via a unique login ID that will be audited and can be traced back to each individual user. The login ID must not give any indication of the level of access that it provides to the system (e.g. administration rights).

System administrators must have individual administrator accounts that will be logged and audited. The administrator account must not be used by individuals for normal day to day activities.

Application and Information Access

Access within software applications must be restricted using the security features built into the individual product. The appropriate department of the software application is responsible for granting access to the information within the system. The access must:

- Be compliant with the User Access Management section and the Password section above
- Be separated into clearly defined roles
- Give the appropriate level of access required for the role of the user
- Be unable to be overridden (with the admin settings removed or hidden from the user)
- Be free from alteration by rights inherited from the operating system that could allow unauthorised higher levels of access
- Be logged and auditable

Policy Compliance

If any user is found to have breached this policy, they may be subject to MRC Print Limited disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from the appropriate person.

Policy Governance

The following table identifies who within MRC Print Limited is accountable, responsible, informed or consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy
- **Accountable** – the person who has ultimate accountability and authority for the policy
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment

Responsible	XXXXXXXXXX
Accountable	XXXXXXXXXX
Consulted	XXXXXXXXXX
Informed	XXXXXXXXXX

Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by the appropriate person.

Key Messages Recap

- All users must use strong passwords
- Passwords must be protected at all times and must be changed at least every 90 days
- User access rights must be reviewed at regular intervals
- It is a user's responsibility to prevent their user ID and password being used to gain unauthorised access to MRC Print Limited systems
- Partner agencies or third party suppliers must not be given details of how to access MRC Print Limited network without permission from the appropriate person
- Partners or third party suppliers must contact the appropriate person before connecting to the MRC Print Limited network