Catena
Inspection & Engineering Services Ltd
Lifting Solutions & Supplies

CHR023 IT and Cyber Policy and Procedure

MARCH 2025 | ISSUE 2

IT Systems Password Policy

Passwords are an essential part of network security, they are the front line of protection of user accounts. A poorly chosen password may result in the compromise of an account and potentially an entire network and associated devices and services.

Effective password controls are in place to ensure that the integrity of all systems and access logins is maintained. The following procedures and practices should be followed to ensure the security and integrity of any accounts.

- All users must ensure their password is not divulged or shared with anyone else
- All users must not create passwords that fall into the category of weak password
- All users **must not** write down and store passwords within the office ie. On paper notes or notebooks.
- Passwords should not be entered into email messages or other forms of electronic communication.
- Temporary password **must** be changes as soon as possible.
- Where possible use a random password generator to create mixed character password with a minimum length of 8chars if MFA is also used
- If MFA is not available a min password length of 12chars must be used

If you are in any doubt that a password may have been compromised this must be changed immediately. You should also inform the IMS Manager / IT Dept to discuss the potential risks involved and if any further action is needed.

Unattended Computer Policy

When leaving your computer unattended, for any amount of time, you need to Lock the screen. Most keyboards have a shortcut button for this, or alternatively you can do this via the Windows icon > Clicking the Power Icon > Clicking Lock

You then need to log in as normal on your return

Business Mobile Phone Policy

Mobile phones issued by the business must have 6 digit PINs in place. It is acceptable to use biometrics to log in. You shall also set the phone to auto lock after 1 minute.

The phone software shall always be updated to the latest available version as software updates are released. If a phone's age means that it can no longer be updated, the company shall replace the mobile phone.

Computer Admin Accounts

Admin accounts have risks associated with their use.

Users should not use local admin accounts for daily activity, this includes the use of email, internet browsing.

Acceptable use of an admin account is for the updating or installation of any software which required admin access, it should only be used for this purpose and not as a user logon account.

Home and Off Site Working

Users should have their computer set to time out when unattended for 5 minutes.

They shall follow the same criteria as in 'IT Systems Password Policy' and the 'Unattended Computer Policy'

If using a laptop, users shall connect to know or secure wi-fi when accessing work related information.

IT Systems Access Requirement

T3 Network Solutions Ltd provide IT support to Catena Inspection & Engineering Services and its employees, as part of this support 'Administrator' access is required to the Catena network and its IT infrastructure.

Access is required but not limited to :

Network Equipment
Desktop and Laptop computers
Server Equipment

Roles and Responsibilities

Breaches or suspected breaches shall be reported to the Managing Director or the IMS Manager

Annex 1

This document is used to track and monitor Administrator computer access

Employee	Device	Desc	Reason	Approved by	Approval Date
Kat Moss	CIS-06-PC	Desktop PC	Company Director	K.Moss	01/10/23
Kat Moss	CIS-KM-LAP	Laptop	Company Director	K.Moss	01/10/23

Approved Application List

Device	Store	App Name	Approved	When	Who
iPhone	iTunes	Outlook App	Yes	01/10/23	KM
iPhone	iTunes	Nest	Yes	01/10/23	KM
iPhone	iTunes	Chrome	Yes	01/10/23	KM
Samsung	Play Store	Hive	Yes	01/10/23	KM
Samsung	PlayStore	Outlook App	Yes	01/10/23	KM
PC	Windows	Chrome	Yes	04/09/23	KM
PC	Windows	Motion	Yes	01/01/24	KM
PC	Windows	Solidworks	Yes	01/10/23	KM