**Clear Quality Limited**

**Information Security**

All Clear Quality Limited staff have a responsibility to safeguard any personal data that we store on company systems, which includes personal information relating to living identifiable individuals such as company employees as well as contact information on member companies and their employees. You may be committing an offence under the GDPR/ Data Protection Act if you don't guard against unauthorised access to, or unlawful processing and accidental loss destruction or damage to personal data.

**Risk management:** Risk management should be used to identify potential information security risks, assessing their likelihood and possible impact and, depending on their seriousness, reduced them to an acceptable level. Risk assessment helps in identifying the risks faced by the business and consequences of losing valuable data or critical systems.

**Visitors Network Access:** Currently the Clear Quality office does take visitors internally; all meetings happen externally to the office. No visitors are given access to the ‘Quality’ network.

**Password Security:** Passwords will be issued to individuals and should be kept confidential. Under no circumstances should passwords be shared with any other individual. Where IT staff require a password to carry out support/maintenance, passwords should be entered by the individual and not passed on to the technician.

* Passwords should not be made common across systems. Unique passwords should be used for each account or system to which you are granted access.
* All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) should be changed on, at least, a periodic basis
* Administration rights should only be granted to IT staff on an as required basis and following permission from the IT Director.
* Passwords should be maintained and regularly changed on laptops and mobile devices.
* Passwords should not be inserted into email messages or other forms of electronic communication.
* All user-level and system-level passwords must conform to the guidelines described below.

Password Construction Guidelines: Passwords are used for various purposes, the more common of which include: -

1. user level accounts
2. web accounts
3. email accounts
4. screen saver protection
5. voicemail password
6. local router logins

Since very few systems have support for one-time tokens, i.e., dynamic passwords which are only used once, employees should be aware of how to select strong passwords.

Strong passwords have the following characteristics: -

• Contain both upper- and lower-case characters (e.g., a-z, A-Z)

• Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&\*()\_+|~-=\`{}[]:";'<>?,./)

• Are at least eight alphanumeric characters long and is a pass phrase (Ohmy1stubbedmyt0e)

• Are not standard words in any language, slang, dialect, jargon, etc.

• Are not based on personal information, names of family, etc.

• Passwords should never be written down or stored on-line

Under no circumstances should passwords be shared with colleagues or anyone outside of the organisation, including administrative assistants or secretaries. There are other, more secure ways of providing access to shared systems such as shared documents or email accounts.

All passwords are to be treated as sensitive and Company Confidential. As a guideline: -

1. Don't reveal a password over the phone to ANYONE. If someone demands a password, refer them to this document or have them call someone in the IT Department
2. Don't reveal a password in an email message
3. Don't talk about a password in front of others
4. Don't hint at the format of a password (e.g., "my family name")
5. Don't reveal a password on questionnaires or security forms
6. Don't share a password with family members
7. Don't reveal a password to co-workers while on vacation
8. Do not use the "Remember Password" feature provided in applications such as internet browsers, MS Outlook email etc.
9. Do not write passwords down and store them.
10. Do not store passwords in a file on ANY computer system, including personal organisers, mobile phone devices or similar devices unless protected with encryption.

Password Changes: Passwords should be changed at least every six months, with the exception system-level passwords which will be changed on a periodic basis by the IT department. If an account or password is suspected to have been compromised, report the incident to the IT Department and change all passwords.

Internet and email issues: The inappropriate use of email and the internet, e.g., using the internet for non-work purposes, can have significant consequences for your business. This could be in terms of:

• damage to business' reputation

• loss of productivity

• increased risk of liability and legal action, e.g., as a result of sexist or racist emails

• increased risk of virus attack

.

Employee training and data security awareness: Clear Quality Limited employees, assessors, clients, and learners should be regularly trained in the use and processing of data to ensure they are aware of data security principles and what actions might infringe on security or confidentiality. This should include anyone who uses IT systems for their work to ensure these systems are operated in a security-conscious manner. Training should include an awareness of what procedures to follow when systems fail.

Awareness training on data security should be communicated to all employees drawing attention to the following area: -

• Train employees to use systems correctly and give responsibility for ensuring their data is backed-up to network drives or removable storage devices

• Data security procedures and principles, obtaining signed declarations from anyone handling sensitive information.

• Business managers and staff should plan for manually contingencies if technology breaks down

• IT best practice and acceptable use around email, software applications, the internet usage, and the use of passwords – drawing employee attention to employment contracts

• To involve employees in a risk assessment and in regular reviews of your procedures

• Protection and principles under the Data Protection Act 1998

Induction training should include a specific reference to Information Security and other IT policies. Refresher training should be included and recorded as a specific item in the annual appraisal’s personal development plans for any staff involved in handling client data.

**Minimizing the risks associated with remote working:**

When you are travelling you should: -

• Never leave equipment unattended in a public place.

• Avoid leaving equipment in your car. If you must do so, make sure it is not visible.

• Use hotel safes to store valuable equipment and information when not in use.

• Avoid displaying any sensitive information on your laptop screen in a public place.

• Avoid using public access to the internet (for example in an internet cafe). Remember computers can store information that has been entered. As a rule, do not use such places if you are handling sensitive information.

When working at home remember to: -

• Ensure that valuable equipment is covered by an appropriate insurance policy.

• Check that your laptop or workstation has adequate, up-to-date virus protection software installed.

• Regularly back up your data. Keep all back-ups safe and secure, preferably away from your usual place of work.

• Destroy records containing sensitive information when no longer required.

• Ensure that valuable equipment and data is locked away when it is not in use for a long period of time.

Insurance: If office equipment is taken off site (e.g., laptop computers) it is the responsibility of the custodian of the equipment to ensure it is suitably insured either through personal insurance or corporate insurance. Many policies will be invalidated if equipment is damaged or lost outside of the insured premises. Specialist insurance advice should be sought.

**Document control**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Document title | Document owner | Signature | Version | Review date |
| Clear Quality Limited General Policy and Procedures | Bethan Rhodes  | A black and white logo  Description automatically generated with low confidence | Oct21 v.1 | Due Oct 22 |
| Clear Quality Limited General Policy and Procedures | Bethan Rhodes | A black and white logo  Description automatically generated with low confidence | Jan22 v.2 | Due Jan 23 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

This document should be a reviewed a minimum of annually by the CEO or the Training & Certification Director.