Be Rota Limited
Security Access Policy
Schedule 3

Be Rota Limited will establish specific requirements for protecting information and information systems against unauthorised access.

Be Rota Limited will effectively communicate the need for information and information system access control.

Purpose

Information security is the protection of information against accidental or malicious disclosure, modification or destruction. Information is an important, valuable asset of Be Rota Limited which must be managed with care. All information has a value to the organisation. However, not all of this information has an equal value or requires the same level of protection.

Access controls are put in place to protect information by controlling who has the rights to use different information resources and by guarding against unauthorised use.

Formal procedures must control how access to information is granted and how such access is changed.

This policy also mandates a standard for the creation of strong passwords, their protection and frequency of change.

1. Scope

This policy applies to all Be Rota Limited's Directors, Departments, Partners, and Employees (including system support staff with access to privileged administrative passwords), contractual third parties and agents of the organisation with any form of access to Be Rota Limited's information and information systems.

2. Definition

Access control rules and procedures are required to regulate who can access Be Rota Limited information resources or systems and the associated access privileges. This policy applies at all times and should be adhered to whenever accessing
Be Rota Limited information in any format, and on any device.

3. Risks

On occasion business information may be disclosed or accessed prematurely, accidentally or unlawfully. Individuals or companies, without the correct authorisation and clearance may intentionally or accidentally gain unauthorised access to business information which may adversely affect day to day business. This policy is intended to mitigate that risk.

Non-compliance with this policy could have a significant effect on the efficient operation of the organisation and may result in a breach of data, financial loss and an inability to provide necessary services to our customers**.**

4. Applying the Policy – Passwords

a. Choosing Passwords

Passwords are the first line of defence for our ICT 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.

i. *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 seven characters.
- Contain a mix of alpha and numeric, with at least one digit
- More complex than a single word (such passwords are easier for hackers to crack).

b. 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 [amend list as appropriate]:

- 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 Be Rota Limited systems.
- Do not use the same password for systems inside and outside of work.

c. Changing Passwords

All user-level passwords must be changed at a maximum of every 90 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 your line manager.

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

d. System Administration Standards

The password administration process for individual Be Rota Limited systems is well-documented and available to designated individuals.

All Be Rota 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.

5. Applying the Policy – Employee Access

a. 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 de-registration of users who no longer require access. These must be agreed by Be Rota 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.

b. User Registration

A request for access to the organisation's computer systems must first be submitted to the Be Rota Limited.

When an employee leaves the organisation, 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 member of the executive team to request the suspension of the access rights via the Be Rota Limited.

c. User Responsibilities

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

- Following the Password Policy Statements outlined above in Section 6.
- 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 human resources of any changes to their role and access requirements.

d. Network Access Control

The use of USB's and Remote Login methods on non-organisation owned PC's connected to the organisation's 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 human resources before connecting any equipment to Be Rota Limited's network.

e. User Authentication for External Connections

Where remote access to the Be Rota Limited network is required, an application must be made via human resources. Remote access to the network must be secured by two factor authentication consisting of a username and one other component.

f. Supplier's Remote Access to the Organisations Network

Partner agencies or 3rd party suppliers must not be given details of how to access the organisations network without permission from human resources. Any changes to supplier's connections must be immediately sent to human resources so that access can be updated or ceased. All permissions and access methods must be controlled by human resources.

Partners or 3rd party suppliers must contact human resources before connecting to the Be Rota Limited network and a log of activity must be maintained. Remote access software must be disabled when not in use.

g. Operating System Access Control

Access to operating systems is controlled by a secure login process. The access control defined in the User Access Management section (section 7.1) and the Password section (section 6) 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.

h. Application and Information Access

Access within software applications must be restricted using the security features built into the individual product. The access must:

- Be compliant with the User Access Management section (section 7.1) and the Password section (section 6) 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.

7. Policy Compliance

If any user is found to have breached this policy, they may be subject to Be Rota 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 member of the executive team.

8. Policy Governance

The following table identifies who within Be Rota 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	Product Manager
Accountable	CEO
Consulted	Executive team
Informed	All team

9. Review and Revision

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