Mayne Island Improvement District

Information Technology Policy - Passwords and File Protection

POLICY STATEMENT

All employees will endeavor to protect all information through the use of passwords and inadvertent access to their files.

OBJECTIVE

- To safeguard District software and data against unauthorized or inappropriate use, modification, copying, disclosure or destruction.
- To eliminate the risk of unauthorized use of workstations by others to send e-mail and or access to the internet.
- To minimize administrative privilege access to prevent the unauthorized installation of software and programs on to Improvement District server accessible computers.

PASSWORDS

- User identification (name) and authentication (password) must be required to access the operating system of all work stations. Some further identification and authentication may be required for other applications.
- The user is responsible for protection of their passwords.
- Users must immediately notify the specified Network Supervisor upon learning that their ID or Password has been compromised; and must immediately change their password(s).
- Passwords must be kept confidential and are not to be shared with others.

LEAVING WORK STATIONS UNATTENDED

- Computer access to confidential information such as personal and sensitive information must be limited. Therefore, computers should not be left unattended without taking appropriate security precautions.
- Use computers' lockout feature to provide reasonable protection from unauthorized uses.
- In cases where confidential information is stored on the local hard drive, use added prevention such as setting file permissions or using password protection for specific files.

ADMINISTRATIVE PRIVILEGES

Administrative privileges shall be limited to the specified Network Supervisor.