

THE CORPORATION OF THE DISTRICT OF SUMMERLAND
POLICY STATEMENT AND REGULATIONS

Number: 1100.4

INFORMATION TECHNOLOGY PASSWORDS AND FILES PROTECTION POLICY

Objective

1. To safeguard corporate Software and Data against unauthorized or inappropriate use, modification copying, disclosure or destruction.
2. To eliminate the risk of unauthorized use of workstations by others to send e-mail and/or access the Internet.

Passwords

1. User identification (name) and authentication (password) must be required to access the operating system of all workstations. Some further identification and authentication may be required for some applications.
2. The user is responsible for protection their passwords.
3. Passwords must be kept confidential and are not to be shared with others.
4. Password selection and the appropriate use should be as follows:
 - At least 5 characters in length;
 - A non dictionary word;
 - A mixture of characters, both upper and lower case, numbers, punctuation and special symbols subject to a history check to preclude reuse.
 - Passwords should be changed every 90 days.

Leaving Work Stations Unattended

1. 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.
2. Use your computer's lockout feature to provide reasonable protection from unauthorized uses.
3. 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.

Adopted October 10, 2000