Rainy River District Social Services Administration Board	Policy Area **HUMAN RESOURCES** Employee Relations
SECURITY AND BACKUP OF DATA	Policy Number HR-3.11

Policy

The Rainy River District Social Services Administration Board (RRDSSAB) secures its network and computer systems in a reasonable and economical manner against unauthorized access and/or abuse, while at the same time making the systems accessible to authorized and legitimate users.

Attempts to violate the provisions of this policy will result in disciplinary action ranging from the temporary revocation of user access to termination of employment and/or appropriate legal actions. The RRDSSAB will cooperate fully with appropriate authorities to provide information related to actual or suspected activity not consistent with the law.

Procedure

RRDSSAB employees protect the confidentiality of their data and will ensure that sufficient security practices are utilized to prevent inadvertent disclosure of personal documents by using a security password.

RRDSSAB employees will not allow anyone other than the designated Network Administrator use of their network account, email account or passwords for any reason, unless so authorized by the respective Manager. Only the Network Administrator has the right to access all network accounts, email accounts and passwords.

Attempts to login to a computer system using another user's account or as a system administrator is strictly prohibited, unless otherwise authorized by the employee's terms of employment, or under the authority of the respective Manager, in order to meet work requirements. Accounts and passwords should not be shared with anybody, unless a group or project account is established for a specific group of users.

RRDSSAB employees are to comply with computer software licensing agreements defined by federal and provincial laws, including copyright

and patent laws.

Documents that are used by a majority of staff will be installed by the designated Network Administrator on the shared network directory or folders for use by all staff members.

RRDSSAB employees are to save documents and files on the Local Area Network (LAN) in their personal directory. Documents and files are not to be saved on a local hard drive. Those employees on stand-alone systems must take precautions to ensure the security and backup of their files.

The designated Network Administrator shall be responsible for backing up the LAN on a daily basis.

Use of memory sticks shall be discouraged, due to unreliability and lack of security. Memory stick storage may be used for temporary, short-term storage only.

In the event an employee is involuntarily terminated and he/she fails to uphold the data security protocol expected by the Rainy River District Social Services Administration Board, he/she will be subject to criminal investigation of his/her actions.

ADOPTION & REVIEW GUIDELINES

Approved by Res. # 100/01 on 20 September, 2001
Reviewed/Revised by Res. #125/04 on 16 December, 2004
Reviewed/Revised by Res. #20/09 on 9 April, 2009

Approximate date of next review: April, 2013

REFERENCES:	***POLICY AREA***	***POLICY NAME AND NUMBER***
	Governance	*G-16.0 Confidentiality*
	Human Resources	*HR-3.2 Employee Files*
	Human Resources	*HR-3.3 Employee Conduct & Performance*
	Human Resources	*HR-6.0 Privacy of Information*
	Human Resources	*HR-6.4 Privacy Breach Protocol*
	Financial	*F-4.13 Retention of Records*