Category:	Administration Manual	**Number: AE0405**	
Subject:	Information Security - End of Day Procedures	**Page:** 1 of 2	
Approved:		**Revised:**	

1.0 POLICY

1.1 Three Links Care Society ("Three Links"), as a public body as defined under the Personal Information Act of British Columbia and the Personal Information Protection and Electronic Documents Act of Canada, must comply with privacy legislation set out at a provincial and federal level.

1.2 Under the service agreement with Vancouver Coastal Health to provide residential care beds, Three Links is also subject to the Freedom of Information and Privacy Act which sets out the access and privacy rights of individuals as they relate to the public sector.

1.3 Three Links is committed to protecting the personal information under its control and to respecting the privacy of residents, family members, staff, contractors and volunteers regarding personal information that is collected, used, disclosed and retained by Three Links.

1.4 To assist in the protection of personal information, at the end of each business day, each staff person will be responsible for implementing the end of day checklist in Section 3.0 prior to leaving work.

1.5 This policy is applicable to Three Links staff, contractors and volunteers.

1.6 The Director of Human Resources is the Privacy Officer for Three Links Care Society and is responsible for maintaining and enforcing this policy.

2.0 DEFINITIONS

2.1 **"Personal information"** means information about any identifiable individual, including employee personal information, financial information and health record information. Personal information can be found on paper documents and on computers.

Category:	Administration Manual	**Number: AE0405**
Subject:	Information Security - End of Day Procedures	**Page:** 2 of 2
Approved:		**Revised:**

3.0 PROCEDURE

End of Day Checklist

1. Clear your desk – remove any documents containing personal information and lock them in a filing cabinet or desk drawer.
2. Remove any documents containing personal information from printers and lock them away in a filing cabinet or desk drawer.
3. Has information been left in meeting rooms? Remember to clean whiteboards and remove flipcharts, papers and notes when they contain confidential or sensitive information. Secure the information in a locked room or cabinet. Log out of any meeting room computer/laptop.
4. Close out all programs on your computer workstation and then RESTART your machine. DO NOT TURN OFF your machine.
5. Taking personal/confidential information out of the workplace is prohibited. Use remote access if working offsite, do not use personal storage devices such as USB sticks, CDs, etc. Remote access is restricted to certain individuals – management team and select contractors.