SECURITY GUIDELINES FOR PRINTERS AND PHOTOCOPIERS

A new set of security guidelines have been released for printers and photocopiers. Staff managing purchasing and disposing of printers and photocopiers should adhere to these guidelines in order to ensure security of the University's data.

ITS strongly encourages purchasing printers and photocopiers with an **encryption** option. Printers and photocopiers with hard drives hold sensitive data and must be treated accordingly in order to minimize information security risks.

1

Purchasing printers and photocopiers with an encryption option:

- **A** — Products with hard drives should have an encryption option and should be configured by the vendor to encrypt by default.
- **B** — If the vendor cannot enable encryption by default, ensure your IT support enables the option upon receipt of equipment.
- **C** — As an alternative, users may also choose a configuration option to automatically over-write data on the hard drive.

2

Purchasing printers and photocopiers without encryption:

- **A** — Ensure the lease agreement stipulates that the machine's hard drive will be destroyed upon return and proof will be provided.
- **B** — If hard drive destruction is not offered by the vendor, request for the hard drive to be wiped instead.
- **C** — Always request proof from the vendor that the drive was properly wiped.
- **D** — If the vendor does not offer either service, request to remove the hard drives at U of T and wipe / destroy them before returning the equipment. This agreement should be in writing.

Questions? Please contact ITS at security.admin@utoronto.ca for any questions, concerns or further guidance.