INFORMATION SECURITY GUIDELINE

Faxing Medium, High or Very High Risk Information

Introduction

1. UBC information that is sent or received via fax is at risk of being intercepted and copied by unauthorized parties. Users have a responsibility to protect this information, especially when it is Medium, High or Very High Risk Information.
2. This guideline has been issued by the Chief Information Officer to supplement the Transmission and Sharing of UBC Electronic Information standard. Compliance with this guideline is recommended, but not mandatory. Questions about this guideline may be referred to information.security@ubc.ca.

General Considerations

3. Since faxing is not an especially secure method of sharing information, senders should consider using more secure ways of transmitting or sharing Medium, High or Very High Risk Information wherever feasible.
4. Any fax machine used to send or receive Medium, High or Very High Risk Information should be located in a place that prevents unauthorized persons from seeing the information. Access to the machine should be controlled.
5. If using pre-programmed fax numbers, regular monitoring should be done to ensure the fax numbers are accurate and up to date.
6. If regularly faxing Medium, High or Very High Risk Information, the sender should consider using secure fax machines that employ encryption or other security measures. For example, if the fax machine has a feature that requires the recipient to enter a password before the recipient's machine will print the fax, the sender should enable that feature.
7. If computers or Mobile Devices are used for sending, receiving or storing faxes:
    a. the sender should create appropriate computer directories and passwords, so that faxes can only be sent, received and accessed by designated Users, using secret passwords;
    b. before faxing Medium, High or Very High Risk Information by computer modem, the sender should check that the recipient's computer is protected in the same way; and
    c. if faxing High or Very High Risk Information then the computer or Mobile Device must be compliant with the Encryption Requirements standard.

Before Faxing Information

8. Before faxing Medium, High or Very High Risk Information, the sender should consider contacting the intended recipient by phone or email to:
    a. confirm the recipient's fax number;
    b. confirm that the recipient is actually the right person to receive the fax;
    c. confirm that the recipient will be there to receive the fax;
    d. confirm that the recipient will take appropriate precautions to protect the information upon receipt; and
    e. ask the recipient to call to confirm receipt of the fax.

When Faxing Information

9. When faxing Medium, High or Very High Risk Information, the sender should stay by the machine at all times during faxing. The sender should retrieve faxed material from the fax machine, not leave it sitting on or near the fax machine.
10. Senders should always use a fax cover sheet containing the following information:
    a. the sender's identification (with call-back particulars);
    b. the intended recipient;
    c. the total number of pages being sent;
    d. a confidentiality clause saying that the faxed material is confidential, is intended only for the stated recipient, and is not to be disclosed to or used by anyone else; and
    e. a request for anyone who receives the fax in error to immediately notify the sender and then return or securely destroy the information, as the sender requests.

After Faxing Information

11. After faxing the information, the sender should review each fax confirmation report at once to be sure the fax went to the right place, checking the number on the report against the recipient's number and verifying the number of pages that were actually transmitted and received.
12. If Medium, High or Very High Risk Information is mistakenly faxed to the wrong person, or is otherwise compromised through faxing, and the information cannot be recalled, then the sender must report this to the Administrative Head of Unit, who will then initiate an investigation and report the incident in compliance with the Reporting Information Security Incidents standard.
13. After faxing information, the sender should securely destroy any copies that are no longer needed.

Related Documents

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems
Transmission and Sharing of UBC Electronic Information standard