Information Technology Security and Privacy Guidelines for Faxing FSU Information Classified as Protected

Florida State University
Information Security and Privacy Office (ISPO)

Guidelines for Faxing FSU Information Classified as Protected

Privacy and safeguarding of information classified as protected needs to be addressed with a unit faxing strategy. Lessons learned from the news headlines and privacy complaint investigation findings associated with faxing has shown that not restricting access to the fax machine and misdialing the fax numbers are the most common mistakes that lead to privacy breaches. Privacy breaches may occur due to the physical location of the fax machine itself. Privacy breaches of this nature are most often the result of personal information being received on unrestricted fax machines that are placed in open areas where people passing by may view the contents of the faxes received or inadvertently pick up a fax that was not intended for them. IP fax technologies present another privacy issue as FSU loses digital control of documents sent to IP fax destinations. In this case, the receivers logical and physical security controls over the IT infrastructure storing and displaying the document must be relied on.

Bottom line, each unit needs to run a risk analysis on each instance of faxing protected information to determine if the receiver has proper controls to protect FSU's information upon receipt. That means matching any legal (HIPAA for covered medical records/ITAR for restricted research data), contractual obligations concerning the data (Nondisclosure agreements), or just using common sense to craft your strategy.

A unit protected data faxing strategy should include:

1) Limit transmission of protected information to only that information needed by the recipient (i.e. Don't send spreadsheets or database printouts including additional data not needed for the business process);

2) Understand legal or contractual restrictions on faxing select protected information;

3) Ensure receiver has a protected area where faxes are received;

4) Mandatory use of a cover page with FSU data sharing restrictions for receiver (**);

5) When a fax number is entered manually (because it is not one of the pre-programmed numbers) the individual entering the number will visually check the recipient's fax number on the fax machine prior to starting the transmission;

6) Check the fax confirmation printout as soon as the fax is transmitted to proof the receivers number (non-IP faxes) and attach confirmation to faxed document;

7) Verifying that the recipient received the fax.

**This FSU protected information is being transmitted for official use only. Don’t leave sensitive information lying around, including on printers, fax machines, or copiers. And in general, don't print restricted data, including screenshots. Store paper documents that include restricted data in a locked filing system.