**Transmission/transportation of sensitive and confidential information**

If you work with sensitive and confidential information, you are responsible for keeping it safe from accidental or intentional compromise. But classified information has little or no value

unless you can share it with others who have a need to know. The responsibility for

safeguarding sensitive and confidential information becomes especially important when you need to transfer it from one person or location to another.

Several considerations come into play throughout the transmission and transportation process.

1. When is it appropriate to transfer classified information electronically?

Transmission and transportation of classified materials is appropriate when:

1. The sender has the authority to share the material
2. The receiver has a legitimate need to know, clearance or access level, and appropriate secure storage for the level of material.
3. What policies govern the transmission of classified information?

Because protecting classified information from improper disclosure is so critical, there are policies and procedures governing how information can be transmitted or transported. Here are a few key points that need to be considered:

1. All off-campus connections to university servers that involve the transmission of sensitive and confidential Information managed by Doane University must be through a secure and approved system (VPN) by Information Technology Services.
2. All Doane University files that contain sensitive and confidential Information that are transmitted or transported off campus or between campuses must be encrypted and must be securely stored on devices owned and approved by Doane Information Technology Services.
3. All Doane University files that contain sensitive and confidential Information shall not be transmitted over any public wireless network.

More information about Doane’s IT Policies and Guidelines can be found:

<https://www.doane.edu/faq/technology-policies-and-guidelines>

What is the process for transmitting sensitive and confidential information?

The process of transmitting or transporting classified material has several phases.

1. First the sender of the information has to determine whether it is appropriate to transmit the materials at all. There are some important considerations you need to think about before you decide to send classified information. For example, is the intended recipient authorized to receive it and will the recipient be able to store it properly?
2. Then you need to make some advance preparations before the transmission. For example, you have to select which method you are authorized to use to transmit the information. In addition, you will need to prepare the materials properly (encrypt) before they can be transported.
3. Once the materials are on their way, there may be some special procedures you need to be aware of. Finally, the recipient has certain responsibilities once the materials arrive at their destination. Here are a few ways to ensure the receiver’s ability to protect the classified information:
   1. For internal transfers, contact your manager or the manager of the unit where you are sending the information.
   2. For external transfers, contact the information security office: infosec@doane.edu

When you have a need to transfer classified materials from one location to another, a variety of authorized methods are available to you.

* 1. Doane File Exchange
     1. What is Doane File Exchange is an online file transfer service provided to Doane University faculty and staff. By using Doane File Exchange, faculty and staff are able to send very large and secure files to Doane University users and off-campus users.
     2. Why should I use Doane File Exchange?

Email is not best suited for sending large files or files containing classified information. Sending sensitive and confidential Information by email exposes the data to two risks:

1) The email could be sent to the wrong person, usually because of a typing mistake or selecting the wrong name in an auto-fill list;

2) The email could be captured electronically enroute.

3) Additionally, using email to send large files can fill your mailbox quickly, and Doane's email has a 20 Megabyte limit on attachment size.

* + 1. To use Doane File Exchange, visit: <http://www.doane.edu/fileexchange>

By using Doane File Exchange, users are able to send secure files up to 500 Megabytes in size. Also, these files are not stored in your mailbox or the recipients' mailbox.

* 1. Email with link to encrypted content
     1. In the body of your email, add a link to the file or folder containing the sensitive or confidential information. The advantage to this approach is that only authorized users will have direct access to the content.
  2. Email and encrypted content
     1. Doane Gmail by itself is not secure. To properly safeguard information sent via email you must encrypt the file using a method approved by Information Technology Services. Even when contents are encrypted, you still run the risks of sending the contents to the wrong person or the email being captured enroute. Passwords of encrypted files should never be shared in the orginating email with the encrypted contents. Ideally that would be provided by another medium phone, mail or at least separate email. Emails with confidential information may only be sent to verified Doane email addresses. They may not be sent to personal email accounts or any account other than the doane.edu domain. If confidential material needs to be shared outside the doane.edu domain, you must use the Doane File exchange or work Directly with Information Technology Services to transfer by secure FTP or another approved method.

If you do need to send confidential information within the Doane domain, here’s how to do it on a Windows machine and on a Mac. The example provided is for a Microsoft word document. A similar process is available for Microsoft Excel. If you need to be able to encrypt a PDF, please contact the helpdesk for an approved encryption utility like WinZip.

**Encrypting a Document in Microsoft Word for Windows**

We are going to be using Microsoft Word 2010 for these screenshots, but the same commands apply for all versions after that. Open an existing Word document or a new document and go to **File** and select **Info**. You will see an option called *Protect Document*.



Click on **Protect Document***,* and you will get this menu:



Once you choose *Encrypt with Password*, Word will prompt you to add a password. Either use something you know you will remember or write it down—there is no way you can recover the document if you forget.



After you choose a password, Word will prompt you to enter it again.



When you try to open the document again, you will get a message informing you the document is password protected.



**Encrypting a Document in Microsoft Word for Mac**

We are using Microsoft Word 2016 for these screenshots, but the same commands should also work for legacy versions. The method is very similar to that of Windows, but the commands appear in different places in the ribbon.

Just as in the Windows version, start by opening an existing Word document or a new one. Go to **Review** and you will see, at the far right of the screen, the **Protect Document** option.



Click that, and it will give you this pop-up:



From there, add a password. As with the Windows version of Word, the program will prompt you to enter the password again.



That’s it. You’re done. When you try to open this document again, you will see this:



If you send this document to someone, they will need the password to open it. Alternatively, on a Mac, you can set it so your recipient can open it without the password, but they will need a password to modify. Just go through the same steps as above, but instead of choosing **Set a password to open this document** choose **Set a password to modify this document**.



There you have it. With a few brief clicks in Windows or Mac, you can increase the security level of a document. Now you have you have been made aware and provided the tool, let’s be sure to safeguard the information.