**STEPS TO WORKING WITH CONFIDENTIAL DATA**

1. Provide confidential information on a need-to-know basis only.

2. Carefully weigh the need for storing, transmitting, and using data against the risk of exposure and the responsibilities for protecting it.

3. Properly secure data you use on a secured server. Avoid storing copies of confidential data on laptops, desktops, smartphones, or portable devices like USB drives.

4. Data are more easily stolen when shared between users, so encrypt confidential data when transmitted.

5. Don’t use open wireless networks when working with confidential data. Unsecured wireless networks, e-mail, and public computers are vulnerable to security breaches.

6. Exercise caution when using cloud computing services such as Google Apps, Google Docs, Gmail, and Microsoft Office Live.

7. Physically lock up hard copies of confidential data when not in use.

8. Lock your computer when not in use or set up a screen saver to require a password.

9. Properly dispose of confidential data as soon as it is no longer needed. Shred papers and sanitize hard drives when disposing or transferring computers.

**WHAT IS A SECURITY BREACH?**

A security breach occurs when:

- An unauthorized person is believed to have gained the ability to access institutional data that are stored on a university data system, or
- A person who is authorized to access the information misuses that data.

**HOW TO REPORT A BREACH**

Any known or suspected compromise of institutional data or suspicious activity should be reported immediately to the MSU Academic Technology Services Help Desk at (517) 432-6200.

Examples of security breaches and how to report them are available in the document “Guidelines for Internal and External Reporting of Data System Security Breaches” at eis.msu.edu/sid.

**OTHER STEPS:**

**PROTECT YOUR COMPUTER**

A computer should be secured before it connects to the network, e.g., virus protection, patches, and a firewall. Take steps to ensure your system is secure. See your local technical staff or supervisor for details and visit tech.msu.edu/secureIT.