CIT/DFA Annual Attestation

This article applies to: DFA-CIT Service Group IT Support

Use Workday to Complete Your Annual Attestation

By clicking “I Agree” in Workday, you are acknowledging that you are bound by university policies as well as applicable federal, state, and local laws. You understand that a violation of these policies or laws could result in disciplinary action up to and including termination. Questions or concerns can be discussed with the Office of Human Resources (Tammy Dibble, td13@cornell.edu).

In addition, central IT employees must follow 9 specific requirements for all personal productivity workstations (desktops and laptops).These requirements extend to any desktop or laptop used to process or store university data. They do not apply to servers, databases, or infrastructure components.

Review These University Policies Annually

Ethical Business and Financial Policies in Support of the Sarbanes-Oxley Act

Sarbanes-Oxley was passed by the U.S. Congress in 2002 to protect investors from the possibility of fraudulent accounting activities by corporations.

> 4.12 Data Stewardship and Custodianship – with special attention to *Access to Confidential University Administrative and Student Data and Information: Acknowledgement and Understanding*

CIT Intranet Articles

DFA-CIT Service Group IT Support Articles

see all

Guides

CIT Operational Procedures for Information Security ("9 Points")

Static (Permanent) Copies

2017 static (permanent) PDF of CIT attestation

2016 static (permanent) PDF of CIT attestation

4.6 Standards of Ethical Conduct

4.14 Conflicts of Interest and Commitment – If you have *any* concerns that one of your relationships may conflict with this policy, please discuss with your supervisor or someone from Human Resources, such as Tammy Dibble, td13@cornell.edu.

3.6 Financial Irregularities

University IT Policies

5.1 Responsible Use of Electronic Communications

5.2 Mass Electronic Mailing

5.3 Use of Escrowed Encryption Keys

5.4.1 Security of Information Technology Resources

5.4.2 Reporting Electronic Security Incidents

5.5 Stewardship and Custodianship of Electronic Mail

5.6 Recording and Registration of Domain Names

5.7 Network Registry

5.8 Authentication of IT Resources

5.9 Access to Information Technology Data and Monitoring Network Transmissions

5.10 Information Security

Follow Operational Procedures for Handling Confidential Data

Confidential data as defined by University Policy 5.10 is names associated with Social Security, credit card, driver's license, and bank account numbers, as well as protected health information as defined under HIPAA.

Everyone using confidential data is obligated to take reasonable measures to secure confidential information, including data stored on both personal and university-owned equipment.

Spirion or another data discovery tool approved by the IT Security Office must be regularly used to scan for confidential data on any university-owned computers and other storage spaces assigned for your use**. You understand that:**

Data discovery tools, like Spirion, cannot find all instances of all types of confidential data. They can only assist in determining whether confidential data is present.

Because of the limitations of data discovery software, you will maintain awareness of data stored on your system and periodically

review your files, including electronic mail, for confidential data.

If you have confidential data and have a business need to continue to store and/or access this data, you are required to contact either Central IT Technical Support or the IT Security Office for further assistance and instruction.

About this Article

Last updated: Friday, June 1, 2018 - 8:58am