Data Governance & Classification Policy 9.1.1.D – Compliance and Remediation

Background

University of Cincinnati personnel are responsible for the protection of sensitive data entrusted to our care; therefore, the Data Governance & Classification Policy was created to help provide simplified guidance and direction for compliance in a complex environment.

Compliance and Remediation Requirements

The Data Governance & Classification Policy requires safeguards for Restricted and Controlled data; see the Minimum Safeguards for details. For requirements related to Controlled Unclassified Information, please follow all safeguards for Restricted data plus additional safeguards as directed by the Office of Information Security. For requirements related to Export Controlled data, please follow all safeguards for Restricted data plus additional safeguards as directed by the Export Controls Office. In support of these requirements, the IT@UC Office of Information Security (OIS) will:

- Provide strategic direction to the university on meeting these requirements.
- Provide education and consulting to the university regarding compliance with this policy.
- Provide remediation training and consulting services to organizations or individuals found to be out of compliance.

The University of Cincinnati reserves the right to suspend access to information systems for suspected violations, pending investigation and resolution. The university reserves the right to terminate access to any user found in violation of its policies, procedures or safeguards.

Breach Notification

In the event of a data breach or a suspected breach certain specific actions must be taken. Refer to the Information Security Incident Management and Response Policy for more complete information. Notification of a breach differs depending on the data type:

- **Controlled Unclassified Information**: Any breach of data in this category must be reported to the unit head and OIS.
    - **Export Control:** Breaches of data in this category must be immediately reported to the unit head, IT@UC Office of Information Security (OIS) and Office of Export Controls.
- **Restricted:** Any breach of data in this category must be reported to the unit head and OIS.
- **Controlled:** Breaches of data in this category must be reported to the unit head, who depending on the severity of the breach, may forward the information to OIS.
- **Public:** No breach notice needed.

Related Links

Data Governance & Classification Policy
Information Security Incident Management and Response Policy

Contact Information

IT@UC Office of Information Security 513-558-ISEC (4732) infosec@uc.edu

History

Issued: 07/01/2009
Revised: 05/30/2014
Revised: 01/25/2017
Revised: 10/25/2017
Revised: 09/26/2018
Reviewed: 09/25/2019
Revised: 09/03/2021