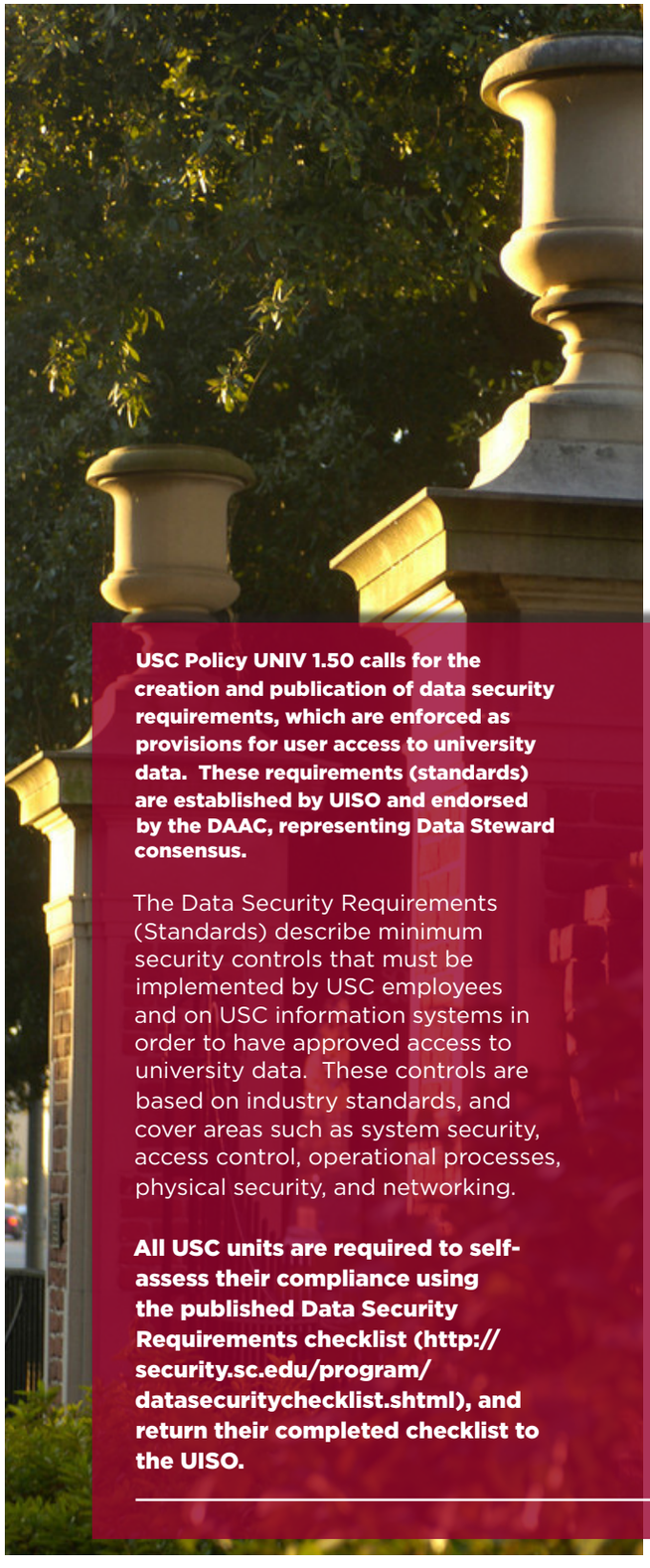


USC Policy UNIV 1.50 calls for the creation and publication of data security requirements, which are enforced as provisions for user access to university data. These requirements (standards) are established by UISO and endorsed by the DAAC, representing Data Steward consensus.

The Data Security Requirements (Standards) describe minimum security controls that must be implemented by USC employees and on USC information systems in order to have approved access to university data. These controls are based on industry standards, and cover areas such as system security, access control, operational processes, physical security, and networking.

All USC units are required to self-assess their compliance using the published Data Security Requirements checklist (http://security.sc.edu/program/datasecuritychecklist.shtml), and return their completed checklist to the UISO.

Resources

To learn more about the USC Information Security Program, including a more detailed breakdown on the roles and responsibilities throughout the incident response process, visit the security website at **http://security.sc.edu**.

For more information on the university's Data Access Policy (UNIV 1.50), see **http://www.sc.edu/policies/univ150.pdf**.

Is there anything else I should know?

Incident-specific costs, such as call center establishment, generating and mailing letters, and other services provided to affected individuals may also be billed to your organization. These costs could reach **up to $25 per affected individual**.

Contact Us

Incident Manager

Incident Tech Lead

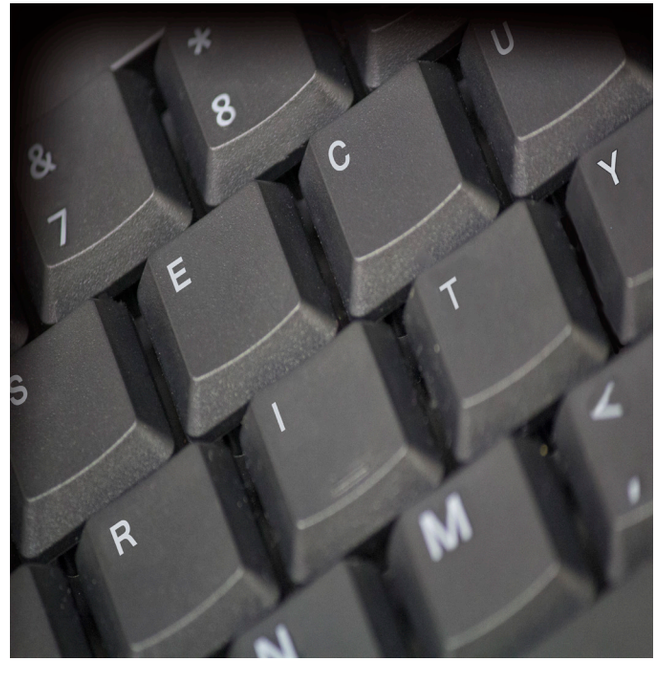
University Technology Services

University Information Security Office

University of South Carolina

Incident Response

A guide to the university's information security incident response process



UNIVERSITY OF SOUTH CAROLINA

Your system has been compromised.

What happens next?

It is vital that you **do not access or alter your system** in any way. This includes powering off the system or disconnecting the network cable before the University Information Security Office (UISO) can retrieve the data we need for our investigation. *Interference with the investigation could lead to disciplinary actions, as outlined by USC policies IT 3.00 and HR 1.39.*

Be sure to **keep your supervisor and appropriate organizational management updated** once the compromise has been confirmed. We want to take every possible step to avoid surprises. UISO will brief Data Stewards/Trustees and other university leadership as appropriate.

The UISO is charged with protecting the university's information assets; our primary concerns are:

- Was the system compromised?
- To what extent was it compromised?
- Were sensitive data compromised or exposed to unauthorized access as a result of this security incident?

When will I know more?

When we have determined how the system was compromised, we will provide you with instructions or recommendations. These recommendations are intended to immediately remove the discovered vulnerability or otherwise minimize further risk of compromise.

An executive summary of our final report will be distributed at the completion of our investigation.

When should the compromised system be disconnected and who has the authority to do so?

The UISO is authorized to take a compromised system offline if university systems or assets are threatened. Data Stewards can also order systems offline if data is believed to be at risk. The business unit (data custodian) may voluntarily disconnect but must coordinate with the UISO to avoid loss of evidence or otherwise impede the investigation.

What is sensitive data?

Sensitive data includes, but is not limited to:

- Private Personal Information (PPI), which can include: full or partial SSN, mailing address or contact information, or other non-public data specific to an individual when last name and first name (or first initial) are also present.
- Healthcare data (may be in the scope of HIPAA)
- Credit card numbers, financial account records, or other payment related data.
- Non-public research data, intellectual property or student academic records.

System Administrator Checklist

Identification

- ☐ Aid in the collection of incident response (IR) data.
- ☐ Fill out the IR questionnaire.
- ☐ Help determine location of sensitive data and how it is used.

Containment

- ☐ Implement a temporary fix for the exploited vulnerability.
- ☐ Help determine if there is a need to disconnect the network device.

Eradication

- ☐ Implement a permanent fix for the vulnerability.
- ☐ Schedule a vulnerability scan on the compromised system, as well as all other systems you manage.

Recovery

- ☐ Implement additional controls that will minimize the risk of future compromises.
- ☐ Restore functionality of the system.

Visit the security website (http://security.sc.edu) for more specific guidelines, recommendations or requirements intended to help you better secure the information assets under your care.