Appendix Data Security

Note: This is an example of using Gen AI to represent documents in multiple ways. Huge caution: Be wary of hallucination so always validate the content. I shared this quickly as a demo.

Document URL:
https://www.ucop.edu/procurement-services/policies-forms/legal-forms-current/appendix-data-security.pdf

---

1. **Mind map by Mapify.so:** https://mapify.so/share-link/BE7foc1ddc
(zoom top right)

---

2. Executive Summary:

The "Appendix Data Security" document outlines the cybersecurity requirements for suppliers working with the University of California (UC). It specifies that suppliers must protect UC's Institutional Information and IT Resources by implementing a comprehensive security plan based on recognized frameworks, such as NIST or PCI DSS. Key responsibilities include performing risk assessments, updating security measures, and reporting breaches or vulnerabilities within 72 hours. The document emphasizes compliance with legal and regulatory standards, limiting access to UC data, and ensuring proper data disposal at the end of the contract. Suppliers are also required to undergo security audits, provide evidence of compliance, and conduct background checks on personnel with access to sensitive data. Non-compliance or security breaches may lead to contract termination and financial liabilities.

3. Summary (by ChatGPT):

The document is an appendix outlining data security requirements for suppliers working with the University of California (UC) on projects involving access to UC's Institutional Information or IT Resources. Below is a summary of the key sections:

1. Purpose and Responsibilities:

- The supplier must adhere to cybersecurity and risk management standards to protect UC's Institutional Information and IT Resources. This includes developing an information security plan based on recognized cybersecurity frameworks and ensuring compliance through third-party reviews or certifications.

2. Defined Terms:

- **Breach**: Unauthorized acquisition or disclosure of Institutional Information or IT Resources.
- **Illicit Code**: Unwanted, hidden, or harmful software that could damage or compromise data or IT systems.
- **Institutional Information**: Any data created or collected by UC.
- **Major Change**: Significant modifications affecting IT Resources, including updates due to technology changes, security incidents, or regulatory shifts.

3. Supplier's Security Plan:

- The supplier is required to establish and maintain a robust security plan that:
    - Protects confidentiality, integrity, and availability of data.
    - Adheres to legal and regulatory requirements.
    - Prevents unauthorized access, changes, or use of Institutional Information.

4. Notification and Reporting:

- Suppliers must report any breaches or security incidents within 72 hours. They must notify UC of major changes or vulnerabilities in their systems and update their security plans accordingly.
- In case of a breach, the supplier must assist UC in the investigation and provide corrective actions.

5. Access Control:

- Suppliers should only access UC data and resources as necessary for providing their services. Unauthorized use for marketing or other purposes is prohibited.

6. Disposal of Data:

- Upon the termination of the contract, the supplier must return or dispose of UC data securely, following UC's disposal standards.

7. Compliance and Audits:

- UC may request evidence of compliance with the security plan, conduct audits, and request reports after security incidents or breaches. Suppliers must cooperate fully with UC during these investigations.

8. Illicit Code Warranty and Background Checks:

- Suppliers must ensure their services are free from malicious or hidden code.
- Background checks are required for any personnel handling sensitive UC data, with results retained for three years.

This appendix is designed to ensure that UC's institutional data is handled securely and that suppliers are held to strict cybersecurity and compliance standards.