Can You Keep a Secret?
Reference Guide

Protecting Data Principles

1. **Authentication - Protect the Credentials**
2. **Authorization - Prevent Unauthorized Access to Sensitive Information**
3. **Accountability - Implement Log Auditing**
4. **Confidentiality - Ensure that data can only be read by intended and authenticated recipients.**
5. **Integrity - Ensure that data is not tampered with or falsified**

Ensure Confidentiality and Integrity

- ✓ Perform Threat Modeling
- ✓ Dell Cryptography Standard
- ✓ Use proven/trusted cryptographic libraries. Non-approved list: Secure Infrastructure (SI) Ready Requirements or Technology Standards
- ✓ Store Secrets Securely
- ✓ Do not display secrets in plaintext
- ✓ Transmit Secrets Securely
- ✓ Ensure Data protection and Privacy
- ✓ Follow best practices for cryptography and security protocols
- ✓ Implement proper Key Lifecycle Management process.

Protect the Credentials

- ✓ Apply Password Protection Mechanism
- ✓ Perform Static Code Analysis
- ✓ Perform Threat Modeling
- ✓ Use a Brute-force Password Tool
- ✓ Ensure proper authentication
- ✓ Perform web security testing (for web applications)
- ✓ Follow Dell's Password Standard
- ✓ Protect against brute force attacks.
- ✓ Support and encourage manufactured-unique or installation-unique secrets.
- ✓ Support changeable secrets/rekey ability.

Prevent Unauthorized Access to Sensitive Information

- ✓ Perform Threat Modeling.
- ✓ Adopt REST Style Architecture, when applicable.
- ✓ Use Recommended Microservices options.
- ✓ Apply least privilege
- ✓ Avoid "Time of Check, Time of Use" (TOCTOU) Issues by performing authorization close to the actual access of sensitive resources.
- ✓ Protect Authentication Tokens/Sessions - must be expirable/revokable, forcing re-authentication.
- ✓ Follow Dell's Access Management Standard.
- ✓ Enforce Proper Authentication
- ✓ Perform testing steps for complete Mediation.

Implement Log Auditing

- ✓ Log all security relevant events, date and time.
- ✓ Do not store confidential information in logs
- ✓ Mask Identifying Information written to a log record.
- ✓ For applications, use the Logging and Alerting Standard.
- ✓ Ensure and validate that log rotation occurs.

Protect Payment Card Information (PCI) & Personally Identifiable Information (PI)

- ✓ Transmitted over a secure (authenticated and encrypted) channel.
- ✓ Stored in an encrypted format using approved algorithms, cipher modes, and key sizes. Sensitive data must never be stored in plaintext.
- ✓ Protect with an access control that ensures a least privilege policy and separates read and write access.
- ✓ Note: Any access to sensitive data MUST BE recorded in an audit log and logs, emails, error messages etc. MUST NOT display sensitive content.
- ✓ Take training on Payment Card Information-Data Security Standard Training.