

The Building Blocks of the Security Policy

1. Principles

2. Policy

This is the statement of intent, the “what” of something we are trying to achieve. This is a **must** do.

3. Standard

This is the rule used to achieve the intent of a policy, the “how” of something we are trying to achieve. This is a **must** do.

5. Job Aid/ Procedure

These are specific sub-items in a standard that require calling out. This is the “how” for a specific use case. This is a **must** do.

6. Guidance

These are the techniques that have been shown to be most effective when implementing a policy, standard, or job aid for given situations. It is how you would choose a specific job aid based on a specific situation. This is a **should** do.

4. Position Papers

This is detailed supporting documentation, evidence, and arguments for a specific policy, standard, or guidance. This is supporting information explaining the “why” of a policy, standard, or guidance.

7. Best Practices

This is a way of doing something that is generally accepted as the best way to perform a task. It is either distributed directly as guidance, or it is used to influence guidance and job aids.

Example: Encryption

1. Principles

2. Policy

All data must be secure in flight.

3. Standard

All network communications will be encrypted using strong public/private key encryption with key lengths over 128 bits.

5. Job Aid/ Procedure

Job Aid 1: Web traffic must use HTTPS / TLS 1.2 or greater.

Job Aid 2: Database connections must enable encryption in the connection string.

Job Aid 3: Raw TCP/IP connections must use strong encryption.

6. Guidance

These are the techniques that have been shown to be most effective when implementing a policy, standard, or job aid for given situations. It is how you would choose a specific job aid based on a specific situation. This is a **should** do.

4. Position Papers

The company will suffer financial and reputational risk due to data loss if it does not follow these standards. Encryption protects the company against eavesdropping attacks on its networks.

7. Best Practices

When encrypting with public/private key pairs, use 1024-bit keys.