MSS Lunch & Learn Series

YALE-MSS-1: System Classification
YALE-MSS-11: Security Training

Jessica Flower
James Tucciarone III
Aaron Wilkey

April 17, 2024
What are the MSS?

• The Minimum Security Standards (MSS) are baseline requirements for securing Yale IT Systems based on risk.

• The MSS apply to any Yale IT System that uses Yale data and/or operates in support of Yale’s mission.
Understanding the MSS

The MSS are broken down into:

• Standard Groups (YALE-MSS-X): These group standards together based on cybersecurity requirements.

• Standards (YALE-MSS-X.Y): Standards tell us we must do to meet that cybersecurity requirement at Yale.

• Controls (YALE-MSS-X.Y.Z): Controls provide details on how you can meet the cybersecurity requirement.

YALE-MSS-1:
System Classification

YALE-MSS-1.1:
Classify the IT System and meet the Minimum Security Standards

YALE-MSS-1.1.2:
Determine your system type
<table>
<thead>
<tr>
<th>STANDARDS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>YALE-MSS-1.1</strong>: Classify the IT System and meet the Minimum Security Standards</td>
</tr>
<tr>
<td><strong>YALE-MSS-1.2</strong>: Apply any additional security requirements required by external obligations</td>
</tr>
<tr>
<td><strong>YALE-MSS-1.3</strong>: Ensure appropriate contracts for all third-party relationships are in place</td>
</tr>
<tr>
<td><strong>YALE-MSS-1.4</strong>: Designate and protect Critical IT Infrastructure</td>
</tr>
<tr>
<td><strong>YALE-MSS-1.5</strong>: Plan for data recovery requirements</td>
</tr>
<tr>
<td><strong>YALE-MSS-1.6</strong>: Plan for meeting and maintaining the security requirements for the IT System</td>
</tr>
<tr>
<td><strong>YALE-MSS-1.7</strong>: Complete a Security Planning Assessment (SPA)</td>
</tr>
</tbody>
</table>
YALE-MSS-1.1
YALE-MSS-1.2

Classify the System and External Obligations

DATA CLASSIFICATION
Determine how sensitive or confidential your data is.

EXTERNAL OBLIGATIONS
Determine if the Yale Data or IT System is subject to any external obligations (e.g., HIPAA, PCI).

AVAILABILITY REQUIREMENT
Evaluate the risk to operations if the IT System becomes unavailable.

The highest risk from the three elements = the risk classification of the IT System
An IT System is being built for the Yale School of Medicine. This system will store personally identifiable patient data (Protected Health Information – “PHI”). The data cannot be unavailable for more than 12 hours.

<table>
<thead>
<tr>
<th>Data Classification</th>
<th>Availability Requirement</th>
<th>External Obligations</th>
<th>Overall Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>PHI is classified by Yale as High Risk</td>
<td>0-8 hours = High Risk 8-24 hours = Moderate Risk &gt; 24 hours = Low Risk</td>
<td>All PHI is regulated by HIPAA</td>
<td>High Risk &amp; HIPAA</td>
</tr>
<tr>
<td>High Risk</td>
<td>Moderate Risk</td>
<td>HIPAA</td>
<td>High Risk</td>
</tr>
</tbody>
</table>
YALE-MSS-1.3

Contracts for Third-Party Relationships

• A data addendum is required for High Risk and Moderate Risk data stored in a vendor’s cloud.

• A Business Associate Agreement (BAA) is required when PHI is disclosed to, created by, or received by a business associate.
Determine the System Type

- Servers
- Endpoints
- Mobile Devices
- Network Printers
Critical IT Infrastructure is defined as an IT system that:

• Unrelated IT systems have a dependency on
• Is complex or specialized in nature and requires special protections beyond Yale’s MSS

This standard enforces extra security controls to protect critical IT infrastructure appropriately.
Plan for Data Recovery Requirements

• Ensure adequate backups of the data the IT System contains.

• Determine the maximum amount of data that can be lost during a disruption before incurring significant impact to operations.
Security planning should include:

1. Classifying the system
   “What do I have?”

2. Knowing your game plan
   “Who is doing what?”

3. Submitting exception requests
   “What is not being met?”
What is a SPA?

The Security Planning Assessment (SPA) is a process to ensure the security of Yale IT Systems. The SPA replaces the old Security Design Review (SDR) process. The SPA process is based on Yale’s Minimum Security Standards (MSS). It ensures you have a plan to operate a secure IT System through the life span of the system.

**MSS Review**
Know your system's risk and apply requirements before requesting a SPA.

**SPA Intake**
Request a SPA and complete a risk assessment of the system.

**Risk Mitigation**
Address specific risks to the system to complete the SPA.
## YALE-MSS-11: Security Training

<table>
<thead>
<tr>
<th>STANDARDS</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>YALE-MSS-11.1: Require security training for all users of Yale Data and</td>
<td>Yale Data and Yale IT Systems</td>
</tr>
<tr>
<td>Yale IT Systems</td>
<td></td>
</tr>
<tr>
<td>YALE-MSS-11.2: Ensure all third parties complete required training</td>
<td></td>
</tr>
</tbody>
</table>
Addendum

- **YALE-MSS-1**: Risk Classification
- **YALE-MSS-11**: Security Training
- **Yale’s Risk Classification Guideline**
- **Contacting Procurement**: Purchasing Intake Portal
- **HIPAA Policy 5033**: Disclosure of PHI to Business Associates
- **Minimum Physical Security Standards for Critical IT Spaces**
- **Applying the MSS to IT Systems**
- **Security Planning Assessment (SPA)**
- **Request an Exception**
- **Contact the Information Security Office**: information.security@yale.edu