Information Security Liaison Program

Initial Meeting – May 24, 2017
Introduction
The UAB ISL Program
Introduction

What is the Information Security Liaison Program?
Security is a team sport.
Collaboration is crucial.

Create a secure computing environment for all UAB members through appropriate policy, training, and technology.

When students, faculty, and staff feel safe in their computing environment, they can work more efficiently without fear of external threats and are at greater liberty to foster new, innovative ideas, with the knowledge that their work is secure.
Information Security Liaison

The scope of responsibilities of the ISLs in each academic and business unit includes, but is not limited, to the following:

• Serving as the primary contact for a department with EISO for information security issues.
• Managing departmental network access authorization, including assigning network addresses, such as TCP/IP addresses, managing the Domain Name System (DNS) requests and local network connectivity.
• Reporting departmental devices that handle Sensitive or Restricted information, such as Social Security numbers, credit card numbers or health records.
• Assisting employees with conducting University business in a secure and compliant manner.
• Reporting and/or assisting with computer security incident response.
• Assist / facilitate the remediation of vulnerability scanning and penetration tests results.
• Participating annually in training specifically designed for ISLs.
Information Security Liaison

The scope of responsibilities of the ISLs in each academic and business unit includes, but is not limited, to the following:

- Serving as the primary contact for a department with EISO for information security issues.
- Managing departmental network access authorization, including assigning network addresses, such as TCP/IP addresses, managing the Domain Name System (DNS) requests and local network connectivity.
- Reporting departmental devices that handle Sensitive or Restricted information, such as Social Security numbers, credit card numbers or health records.
- Assisting employees with conducting University business in a secure and compliant manner.
- Reporting and/or assisting with computer security incident response.
- Assist / facilitate the remediation of vulnerability scanning and penetration tests results.
- Participating annually in training specifically designed for ISLs.
Information Security Liaison

The scope of responsibilities of the ISLs in each academic and business unit includes, but is not limited, to the following:

• Serving as the primary contact for a department with EISO for information security issues.

• Managing departmental network access authorization, including assigning network addresses, such as TCP/IP addresses, managing the Domain Name System (DNS) requests and local network connectivity.

• Reporting departmental devices that handle Sensitive or Restricted information, such as Social Security numbers, credit card numbers or health records.

• Assisting employees with conducting University business in a secure and compliant manner.

• Reporting and/or assisting with computer security incident response.

• Assist / facilitate the remediation of vulnerability scanning and penetration tests results.

• Participating annually in training specifically designed for ISLs.
Information Security Liaison

The scope of responsibilities of the ISLs in each academic and business unit includes, but is not limited, to the following:

- Serving as the primary contact for a department with EISO for information security issues.
- Managing departmental network access authorization, including assigning network addresses, such as TCP/IP addresses, managing the Domain Name System (DNS) requests and local network connectivity.
- Reporting departmental devices that handle Sensitive or Restricted information, such as Social Security numbers, credit card numbers or health records.
- Assisting employees with conducting University business in a secure and compliant manner.
- Reporting and/or assisting with computer security incident response.
- Assist / facilitate the remediation of vulnerability scanning and penetration tests results.
- Participating annually in training specifically designed for ISLs.
Information Security Liaison

The scope of responsibilities of the ISLs in each academic and business unit includes, but is not limited, to the following:

• Serving as the primary contact for a department with EISO for information security issues.
• Managing departmental network access authorization, including assigning network addresses, such as TCP/IP addresses, managing the Domain Name System (DNS) requests and local network connectivity.
• Reporting departmental devices that handle Sensitive or Restricted information, such as Social Security numbers, credit card numbers or health records.
• Assisting employees with conducting University business in a secure and compliant manner.
• Reporting and/or assisting with computer security incident response.
• Assist / facilitate the remediation of vulnerability scanning and penetration tests results.
• Participating annually in training specifically designed for ISLs.
The scope of responsibilities of the ISLs in each academic and business unit includes, but is not limited, to the following:

- Serving as the primary contact for a department with EISO for information security issues.
- Managing departmental network access authorization, including assigning network addresses, such as TCP/IP addresses, managing the Domain Name System (DNS) requests and local network connectivity.
- Reporting departmental devices that handle Sensitive or Restricted information, such as Social Security numbers, credit card numbers or health records.
- Assisting employees with conducting University business in a secure and compliant manner.
- Reporting and/or assisting with computer security incident response.
- Assist / facilitate the remediation of vulnerability scanning and penetration tests results.
- Participating annually in training specifically designed for ISLs.
Information Security Liaison

The scope of responsibilities of the ISLs in each academic and business unit includes, but is not limited, to the following:

- Serving as the primary contact for a department with EISO for information security issues.
- Managing departmental network access authorization, including assigning network addresses, such as TCP/IP addresses, managing the Domain Name System (DNS) requests and local network connectivity.
- Reporting departmental devices that handle Sensitive or Restricted information, such as Social Security numbers, credit card numbers or health records.
- Assisting employees with conducting University business in a secure and compliant manner.
- Reporting and/or assisting with computer security incident response.
- Assist / facilitate the remediation of vulnerability scanning and penetration tests results.
- Participating annually in training specifically designed for ISLs.
Information Security Liaison

The scope of responsibilities of the ISLs in each academic and business unit includes, but is not limited, to the following:

• Serving as the primary contact for a department with EISO for information security issues.
• Managing departmental network access authorization, including assigning network addresses, such as TCP/IP addresses, managing the Domain Name System (DNS) requests and local network connectivity.
• Reporting departmental devices that handle Sensitive or Restricted information, such as Social Security numbers, credit card numbers or health records.
• Assisting employees with conducting University business in a secure and compliant manner.
• Reporting and/or assisting with computer security incident response.
• Assist / facilitate the remediation of vulnerability scanning and penetration tests results.
• Participating annually in training specifically designed for ISLs.
Key Responsibilities

• Reporting departmental devices that handle Sensitive or Restricted information, such as Social Security numbers, credit card numbers or health records in the IP Address Management (IPAM) System.
• Reporting and/or assisting with computer security incident response.
• Assisting in Vulnerability Management Program (vulnerability scanning and penetration testing).

Training Session for IPAM, Incident Response and Vulnerability Management planned for next month.
ISL Resources

- ISL Website – [http://www.uab.edu/it/home/isl](http://www.uab.edu/it/home/isl)
- Ongoing Training Sessions
- Tools
Agenda

Data Reduction
Reducing PII
Data Reduction Efforts
Data Reduction as a protection mechanism

Requirements based on data classification

- **Public**
  - No special requirements.
- **Sensitive**
  - Remove what can be removed and follow the Data Protection Rule.
- **Restricted**
  - Only keep what you need. Must be in an approved environment and follow Data Protection Rule.

References:
- Data Classification Rule
- Data Protection Rule
- Records Retention Policy
- Records Retention Schedule
Data Reduction Phases

**Planning**
Where to look, for what and how. File shares, email, workstations, laptops, etc.

**Discovery**
Manual Tool like Spider, Spirion.

**Inventory**
Inventory the data in your area and categorize it by data classification.

**Remediation**
Determine what to do with it: Delete, reduce, move to an approved environment.

**Continuous Monitoring**
Develop processes and procedures within your area of how and where to store data. Scan to validate.
Data Reduction Resources

• Data reduction site URL <Coming Soon>
• Tools you can use to scan for PII
• REMEMBER:
  • Only keep what you need!
  • Redact documents as a mitigation
  • Follow UAB policies, standards and procedures
  • Assist in educating UAB community regarding responsibilities and procedures for safely handling data.
Confidential records counts

• Once you have determined what data you have and where:
  • Keep inventories and confidential records count up-to-date
  • Use easy math, e.g., you keep records for 7 years, have an average of 1,000 students per year – FERPA count is 7,000
  • Only keep what you need
  • Redact documents as a mitigation – if you need the report but not the SSN included, redact the SSN
  • Move Restricted data to the data center
Agenda

Policies & Standards
Updates & New
Policies & Standards

- Updating some existing policies & standards
- Sunsetting some policies & standards
- Creating new, needed policies & standards
## Policies and Standards

### Imperative 1: Create a secure computing environment for all UAB members through appropriate policy, training, and technology.

#### Objective 1: Protect university and faculty, student, and staff confidentiality.

<table>
<thead>
<tr>
<th>No</th>
<th>Tactics</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td><strong>Tactic 1.1:</strong> Construct a set of policies and standards to enable a secure computing environment. Policies should be lean and authorize development of Standards that can undergo a more rapid development and update cycle.</td>
</tr>
<tr>
<td>1.1.a</td>
<td>Establish a Data Access Policy.</td>
</tr>
<tr>
<td>1.1.b</td>
<td>Establish an Access and Authentication Policy.</td>
</tr>
<tr>
<td>1.1.c</td>
<td>Establish an Acceptable Use Policy.</td>
</tr>
<tr>
<td>1.1.d</td>
<td>Establish a Data Classification and Protection Standard.</td>
</tr>
<tr>
<td>1.1.e</td>
<td>Establish a Password/Authentication Standard.</td>
</tr>
<tr>
<td>1.1.f</td>
<td>Establish an Access Management Standard.</td>
</tr>
<tr>
<td>1.1.g</td>
<td>Establish a Network Device Standard.</td>
</tr>
<tr>
<td>1.1.h</td>
<td>Establish a Sensitive Device Standard</td>
</tr>
<tr>
<td>1.1.i</td>
<td>Establish Awareness/Training Standards.</td>
</tr>
<tr>
<td>1.2</td>
<td><strong>Tactic 1.2:</strong> Assess security policies and standards enacted across UAB Campus and Health System.</td>
</tr>
<tr>
<td>1.2.a</td>
<td>Determine policies and standards that need to be updated, go through a sunsetting process, or new ones that need to be created.</td>
</tr>
<tr>
<td>1.2.b</td>
<td>Publish up-to-date list of security policies and standards.</td>
</tr>
<tr>
<td>1.2.c</td>
<td>Identify or define escalations &amp; enforcements within each policy or standard.</td>
</tr>
</tbody>
</table>
Policies and Standards Process

**Policies**
- Initial Policy Draft
- Information Security Advisory Council (ISAC) reviews and makes recommendations
- Proposed Policy then submitted to University Compliance for broad review and President’s approval

**Standards**
- Initial Standard Draft
- Volunteer ISL sub-group reviews and makes recommendations
- Proposed Standard submitted to Dr. Curtis A. Carver, Jr. for approval
Policies and Standards Resources

- http://www.uab.edu/it/home/it-related-policies
- Box.com collaboration site
Next Up

<table>
<thead>
<tr>
<th>Training Session</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident Response, Vulnerability Management &amp; IPAM</td>
<td>June 2017</td>
</tr>
<tr>
<td>IPAM User’s Session</td>
<td>July 2017</td>
</tr>
</tbody>
</table>
Thanks for participating and we look forward to working with you!

Knowledge that will change your world