Memorandum

21 March 2017

From: Dr. Curtis A. Carver Jr., Vice President for Information Technology and Chief Information Officer
Subject: Information Security Liaison Designations

As part of UAB’s initiative to reduce risk and create a secure computing environment, my office is instituting the Information Security Liaison (ISL) program. This program will establish a designated point of contact for security within each University academic and business unit. An important initial step of the liaison program will be to reduce the number of sensitive records and/or servers under his/her purview.

In the 2016 UA System-wide Inventory of Servers and Unique Sensitive Records Report, UAB was an outlier compared to the other UA System Institutions having reported the highest percentage of Sensitive records on distributed servers. This puts UAB at greater risk, which increases the need for greater security controls and more consistency in process and procedure.

We do not have a record of declarations for your academic/business unit in the 2016 UA System-wide Inventory of Servers and Unique Sensitive Records Report. If you have sensitive records, it is important that those sensitive records and systems be declared for your academic/business unit for subsequent Board reports.

In coordination with the UA System Office, President Watts, and the Department of Internal Audit, we have established a goal of reducing the number of Sensitive Records in Distributed Servers by 25% for 2017 and 10% annually thereafter. Below is a chart outlining the University’s goals for the reduction of sensitive information within distributed servers.
<table>
<thead>
<tr>
<th>Year</th>
<th>Total PII Records Reported in distributed units</th>
<th>% reduction of PII in distributed units</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016</td>
<td>316,700</td>
<td></td>
</tr>
<tr>
<td>2017</td>
<td>236,580</td>
<td>25%</td>
</tr>
<tr>
<td>2018</td>
<td>213,000</td>
<td>10%</td>
</tr>
<tr>
<td>2019</td>
<td>192,000</td>
<td>10%</td>
</tr>
<tr>
<td>2020</td>
<td>172,000</td>
<td>10%</td>
</tr>
</tbody>
</table>

In support of our risk reduction efforts and the liaison program, please designate employees as primary and secondary Information Security Liaisons for your academic / business unit that will serve as a point of contact to the Enterprise Information Security Office (EISO). For UAB covered entities, this designation may overlap with the UAB Health System Entity Security Coordinator designation.

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 critical, 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.
- Participating annually in training specifically designed for ISLs.

Please provide your ISL designations by email to Cindy Jones at security@uab.edu by April 30, 2017.

If you have any questions, please contact me at carverc@uab.edu or Brian Rivers, chief information security officer, at cbrivers@uab.edu. You can also check our frequently asked questions for the ISL program.