Information Security Incident Protocol

This protocol is intended to assist University administration and staff in the event that University data is compromised.

University data is defined as: Items of information that are collected, maintained, and utilized by the University for the purpose of carrying out institutional business subject to or limited by any overriding contractual or statutory regulations. University data may be stored in any number of formats, including but not limited to electronic, paper, graphics, photographs, video, audio or metadata.

Incident Response Process:

1. A potential or actual compromise of University data or of a system containing University data is uncovered by or reported to a University office or department.

2. The potential or actual incident should be reported to Chief Information Security Office (CISO) in UITS or the Privacy Officer in OACE, *immediately*.

3. The Privacy Officer and CISO will coordinate as appropriate to collect information regarding the compromise and determine the appropriate course(s) of action to investigate the compromise.

4. If it is determined that University electronic devices (e.g., computers, mobile devices) or paper records have been stolen or otherwise have gone missing, the Privacy Officer and/or CISO will report the loss to the University Police.

5. The Privacy Officer and/or CISO will coordinate with appropriate University departments for investigation, containment, preservation, forensics and/or protection of sensitive data. As part of this process, the Privacy Officer and/or CISO will determine what sensitive and/or personal data may have been compromised.

6. As information becomes available over the course of the investigation, the CISO and/or Privacy Officer will determine whether it appears that sensitive personal information may have been exposed and/or breached.

7. If the CISO and Privacy Officer reasonably believe that a breach may have occurred, the CISO and Privacy Officer will contact the Office of the

General Counsel to discuss the actual or potential breach, legal obligations and proactive strategies.

8. If it is determined in conjunction with the Office of the General Counsel that a data breach has occurred, the Privacy Officer and CISO will contact members of the Security Incident Team (SIT) described below to discuss available information, and to begin troubleshooting how to handle the breach.

9. The SIT is comprised of the following standing members:

    - CISO
    - Privacy Officer
    - General Counsel
    - Chief of Staff
    - Deputy Chief of Staff
    - University Communications
    - Dean, Director or Department Head of the area where the breach is determined to have occurred

    Other members of the University community will be asked to collaborate or participate where appropriate.

10. Once enough information about the situation is known and/or the extent of the breach has been determined, the Privacy Officer and CISO will collaborate with the Office of the General Counsel and appropriate members of the SIT to determine who needs to be notified about the breach, how individuals impacted by the breach should be notified and what, if any, services should be offered to the individuals impacted by the data breach to help protect themselves from potential or actual identity theft. As part of this analysis, the Privacy Officer will coordinate with the Office of the General Counsel to review applicable state (CT and any other applicable state) and federal privacy, data security and breach notification laws, standards and best practices.

11. The SIT will then formulate a plan of action to comply with applicable requirements of such laws, standards and best practices.

12. If it is determined that notification and credit monitoring protection is appropriate and/or required, the Privacy Officer will engage the

University's designated vendor to provide notification and credit monitoring services on the University's behalf. Unless an exception is determined to be appropriate by the SIT, the office or department responsible for the data that was lost or breached shall be responsible for the costs associated with remediating the breach, including but not limited to notification and credit monitoring services.

13. Where required by state and or federal law, the Privacy Officer will coordinate with the appropriate members of the SIT to ensure that the required state entities, federal government entities and/or credit bureaus (e.g., attorneys general, other state agencies, FTC, DHHS) are notified of the breach and who has been impacted as well as the University's course of action related to managing the breach.

14. Where appropriate, the Privacy Officer, CISO and/or Office of the General Counsel will contact the Connecticut Office of the Attorney General (through the AG's Privacy Taskforce), the Governor's Office and/or any other appropriate State Officials to inform them about the breach.

15. Where necessary or appropriate, the SIT will expeditiously collaborate to develop press releases and letters to affected individuals (by email and/or U.S. post).

16. Where appropriate, the CISO will coordinate with University Communication to create web page(s) with information regarding the breach and how individuals can take steps to protect themselves.

17. The SIT will also designate a single point of contact to address questions/concerns of individuals concerned about the breach. The SIT may decide to set up special toll-free number phone line for individuals to call with questions/concerns where required and/or appropriate. The Privacy Officer will ensure that appropriate offices (i.e., University switchboard, University Communications, Office of the President, office who lost or who is responsible for the data that has been compromised) are made aware of the single point of contact to whom questions/concerns should be directed.

18. In the course of managing and remediating the breach, as expeditiously as possible:

    - The Privacy Officer will work with Purchasing and the office or department responsible for the costs of remediating the breach to process necessary paperwork to engage the University's

designated vendor to provide notification and/or credit monitoring services.

- The Privacy Officer will work with the vendor to process any appropriate paperwork (i.e., SOW, PO, etc.) to engage the vendor's services.

- The Privacy Officer will work with appropriate University staff, the Office of the General Counsel and the vendor to draft notification letters and where appropriate, FAQ's regarding the incident.

- The Privacy Officer and/or CISO will work with appropriate University staff to collect the names and last known addresses of individual who will need to be notified.

- Notification letters will be sent to impacted individuals or organizations via First Class Mail, email and/or other methods required by law.

- Press releases will be finalized and issued by University Communications where appropriate. The main University website(s), faculty/staff webpage student information webpage will include link to press releases.

- A special website containing information regarding the breach, how to get more information, and how to protect one's credit will be posted as appropriate by University Communications and/or the UITS Information Security Office.

19. A mechanism for logging calls and/or inquiries received, as well as responses and/or assistance given, shall be created and implemented.

20. Once proper notifications have been sent and posted and the matter has been contained and handled, debriefing meeting(s) should be held with all of the individuals involved in the breach investigation, management and remediation. Additional follow-up activities should occur as appropriate.