UCI Division of Finance and Administration

Data Security Incident Response Plan

How do I report an actual or suspected security breach?

*Contact the OIT Help Desk at (949) 824-2222 to report that an actual or potential data breach has occurred and request immediate notification of the **OIT Security Team**. Also, please send any available detailed information to security@uci.edu.*

AND

Contact Jenifer Swann, Integrated Systems Development Manager, Division of Finance and Administration at (949) 824-6956, jmnorthr@uci.edu or, Rick Coulon Associate Vice Chancellor of Campus Operations, Division of Finance and Administration at (949) 824-5108, rcoulon@uci.edu.

For additional information and resources related to cybersecurity visit: https://security.uci.edu/

What else do I need to know?

Cyber security are the techniques of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation. Some common types of cybersecurity issues include malware, phishing and SQL Injection.

Malware

Malware refers to various forms of harmful software, such as viruses and ransomware. Malware can do many things from taking control of the machine, to monitoring actions and keystrokes, to silently sending all sorts of confidential data from the computer or network to the attacker's home base. Various methods are used to accomplish this, but at some stage it often requires the user to take an action to install the malware. This can include clicking a link to download a file, or opening an attachment that may look harmless (like a Word document or PDF attachment), but actually has a malware installer hidden within.

Phishing

In a phishing attack, an attacker may send the user an email that appears to be from a trusted source. The email will seem legitimate, and it will have some urgency to it (e.g. fraudulent activity has been detected on your account). In the email, there will be an attachment to open or a link to click. Opening the malicious attachment may trigger installation of malware on the computer. Another type if phishing may send the user to a legitimate-looking website that asks for your user name and password and will actually capture the user's credentials. In order to combat phishing attempts, understanding the importance of verifying email senders and attachments/links is essential.

SQL Injection

SQL injection attacks specifically target servers that store critical data for websites and services that use SQL to manage the data in their databases, using malicious code to get the server to divulge

information it normally wouldn't. This is especially problematic if the server stores private information, such as credit card numbers, usernames and passwords (credentials), or other sensitive or personal identity information.

Storing and Sharing Data

There are times when personal data from PPS or other systems needs to be provided to co-workers outside of having system access. When doing so it is vital for us to understand how to store and share that information securely. Information that is not properly secured could result in significant fines, penalties, regulatory action, or even civil or criminal violations.

What data do I need to be concerned about?

OIT has categorized restricted data and information risk as low, medium, and high. This information needs to be secure, whether in storage or when being transmitted to others. Some examples of this data include:

- Personally Identifiable Information (names associated with SSN, driver's license numbers, home address, etc.)
- Information contractually identified as restricted
- Court-ordered settlements
- Credit card information
- Other UCI proprietary data that needs to be secured (contracts, bids, research, etc.)

For a more extensive list of restricted data visit:

http://security.uci.edu/security-plan/plan-classification.html

Where do I find out more information about whether my information is properly secured?

The Office of Information Technology provides information security services to the University of California, Irvine.

To request vulnerability assessment or security review services, complete the request form and email it to security@uci.edu for consideration. To inquire about other services or to contact the Security Team, please call the OIT Help Desk at (949) 824-2222 or send an email to oit@uci.edu.

How do I send a file with restricted data?

If High Risk data must be transmitted, a combination of WebFiles and a file encryption tool should be used to securely store and transfer the data between users. **Do not send the data as email attachments**. In general, it is good practice to exchange data using WebFiles even when data elements that are sensitive but not of High Risk are involved. Instruction on how to access and use WebFiles is available at http://www.oit.uci.edu/webfiles/. OIT supported clients may contact the OIT Helpdesk for assistance and to request WinMagic to be installed for file encryption.

For additional information and resources related to cybersecurity visit: https://security.uci.edu/.