UC RIVERSIDE Academic Senate

COMMITTEE ON INFORMATION TECHNOLOGY

To: Senate Colleagues

From: Ilya Brookwell, Chair Committee on Information Technology

RE: UCOP Cyber Security Mandate

Monday, April 28, 2025

Dear Colleagues,

This document is intended to encourage your ongoing participation as senate colleagues in the shared governance of our university. The following is a summary of the capabilities and limitations that we at Senate IT gathered from an internal UCR ITS White Paper. Please note that the call for cybersecurity plans was mandated from the University California Office of the President, and we were informed that these plans are not subject to senate review. Our role and capacity as a committee is to oversee plans and to generate critical feedback, not in this case to participate in joint decision making. That said, our committee has discussed and communicated the serious need for ongoing checks and balances towards privacy, functionality and effectiveness as well as the consequences for IRB and research data governance. Please do address your further questions and concerns to those who implemented these systems and to those with the authority to change them, namely Information Technology Solutions - UC Riverside and the University California Office of the President respectively. We will do the same.

Notes Cybesecurity White Paper (with clarification in bold text)

(1) UCR Security Toolset Purpose

UCR aims to maintain a secure digital environment for faculty, staff, and students.
The toolset is part of a plan to meet UC Office of President's cybersecurity mandate by May 2025. Installation of the UCR Security Toolset is required on all devices intended for university work (personal computers, laptops, desktop either university owned or ‘bring your own device’). iOS and Android devices (your phones and tablets) are currently excluded from the mandate.

The security tools function in very specific ways as follows:

(2) NinjaOne Overview

NinjaOne is a cloud-based endpoint management platform for managing and securing devices. It does the following:
- tracks devices connecting to UCR networks.

- automates critical security tasks including and **limited to patching/updating other security tools** and enforcing security configurations (the toolset is limited to NinjaOne, Trellix and Qualys).
- Reports additional system vulnerability based on a known system vulnerability list.

(3) Trellix Overview

Trellix is an endpoint detection and response (EDR) solution that protects against known and unknown threats. It does the following:
- provides real-time monitoring and automated responses to security events (a known or unknown threat is detected)
- The tool collects data for forensic analysis in case of security incidents. ***No 3rd party outside UC has access or can see this data. Only a very limited specialized team within UCR ITS has access to review data in order to address the security risk.**
- ITS only reviews data on an active incident (where an issue comes up). Human monitoring is only used in threat cases.
- Data retention is not permanent (ITS currently retains data for 1 year on a protected *Google Chronicle* database).
- Does not necessarily replace virus and firewall applications.

(4) Qualys Overview

Qualys is a cloud-based vulnerability management tool that identifies vulnerabilities in larger networked systems environments. It does the following:
- provides real-time visibility on all devices connected to a network
- helps in proactive identification and remediation of vulnerabilities affecting the health of the larger network.
- is a tool that captures detailed asset configuration data and is more concerned with the network health than individual files and end-user system health.

(5) Data Access and Incident Response

UCR prioritizes the privacy and security of data collected by the Security Toolset. Access to data is controlled under the principle of least privilege. The principle of least privilege is an information security concept which maintains that a user or entity should only have access to the specific data, resources and applications needed to complete a required task. The authorized user is given the minimum levels of access needed to perform their job functions. Data authorization is managed ultimately by the CIO who reports directly to the Chancellor.

A comprehensive **Incident Response Plan is in place to address security incidents by a limited internal UCR ITS team.** The stated goal is for ITS to be able to respond and enable end-users back on the network with a minimal turnover time and in just a few hours. Currently, however, it can take up to 48 hours to restore a locked-out user.

Thank you for your interest in understanding this complicated and technical policy. The Senate Committee on Information Technology aims to share all information about the policy and operations of ITS at UC Riverside. We serve the faculty, staff and students both at the local and UC system-wide levels.