OIT Behind the Scenes Webinar Series presents

Ask Me Anything: UC Information Security Policy (IS-3)

with interim
Chief Information Officer
Nick Dugan

Setting Expectations

Lights!

- Camera & Audio controlled bye the hose

Action!

- Enter your questions in the Q&A box

Camera!

- Recorded Session

Cut!

- Feedback requested!

Nick Dugan

Interim Chief Information Officer

BFB-IS-3 Overview

- What is IS-3?
- Why should I care?
- IS-3: A History
- UC Merced implementation: current state

BFB-IS-3

IS-3 is a systemwide policy that defines responsibilities and requirements for:

- Protecting confidentiality of UC data
- Maintaining the integrity of all data created, received or collected by UC (Institutional Information)
- Meeting legal and regulatory requirements
- Ensuring timely, efficient and secure access to information technology resources

Why Should I Care?

Everyone that works for UC Merced has a stake in this policy.

Examples:

- Protecting institutional information
- Following minimum security standards
- Reporting security incidents or gaps in controls
- Completing mandatory training

Policy History

Originally developed in 2009, the process to overhaul the policy began in 2016.

- Catalyst – UCLA Health breach in 2015 (4.5 million patient records)
- Charge – create a modern, risk-based policy to guide UC location cybersecurity programs
- Approved – October 2019
- Adoption - Ongoing

UC Merced Implementation

Start at the center and work our way out

- Develop and implement compliance plan for central IT resources
- Establish procurement and supply chain procedures to ensure supplier compliance
- Implement security measures for end-user devices
- Inform campus units of their roles and responsibilities
- Engage research faculty to ensure compliance

IS-3: Key Policy Elements

ROLES

- Chief Information Security Officer – CISO
- Institutional Information Proprietor
- Unit Head
- Unit Information Security Lead
- Workforce Manager
- Workforce Member
- Researcher
- Service Provider

Data Classification

• P1 • P2 • P3 • P4

Minimum Security Standards

Risk Assessment & Treatment

IS-3 Roles:

CISO

Chief Information Security Officer

Responsible for security functions throughout a Location, including assisting in the interpretation and application of IS-3.

Welcome Jackson Muhirwe, UC Merced CISO!

IS-3 Roles:

Unit Head

1. A Dean, Vice Chancellor, or similarly senior role who has the authority to allocate budget and is responsible for Unit performance.
2. In some situations, the following senior roles may also be Unit Heads: department chairs, assistant/associate vice chancellor (AVC), principal investigators, directors, senior directors, or senior managers.

UC Merced Status – informing and educating identified Unit Heads of their role and responsibilities.

IS-3 Roles:

Other Key Roles

Workforce Member - An employee, faculty, staff, volunteer, contractor, researcher, student worker, student supporting/performing research, medical center staff/personnel, clinician, student intern, student volunteer, or person working for UC in any capacity or other augmentation to UC staffing levels.

Workforce Manager - A person who supervises/manages Workforce Members or approves work or research on behalf of the University.

Researcher - A UC faculty member conducting research on behalf of UC. Also a Workforce Member.

Data Classification

Institutional Information and IT resources must be protected according to their classifications.

IS-3 defines four "Protection Levels" to guide the secure storage and processing of Institutional Information.

Data Classification:

P1

Public *information or information intended to be readily obtainable by the public.*

Example: Information hosted on a public website

Requirements:
Integrity and availability are the primary protection concern for P1 data

Data Classification:

P2

Internal *information and IT resources that are generally not intended for public use or access but are not otherwise protected by statue, regulation, or contractual obligations. Minimal privacy or reputational risk.*

Examples: Routine emails and business records; non-public research using publicly available data; exams (questions and answers)

Requirements:
Access should be controlled and information shared on a need-to-know basis

Data Classification:

P3

Proprietary information whose unauthorized disclosure or modification could result in moderate fines, penalties or civil actions. Unauthorized release could have moderate impact on privacy or result in moderate financial loss.

Examples: Student records; personnel records; research information classified P3 by IRB; data related to animal research projects

Requirements:
Must be encrypted when transmitted and when stored on portable media or computing devices.

Data Classification:

P4

Information protected by ***statutory***, ***regulatory***, *or* ***contractual*** obligations whose disclosure or modification could result in significant fines, penalties, regulatory action, or civil/criminal violations. Risk of significant harm to UC personnel/affiliates or reputational damage.

Examples: Personally Identifiable Information (PII); Personal Health Information (PHI); passwords, PINs, and passphrases; human subject research data

Requirements:
Must be encrypted at all times, systems must meet all minimum security standards and have a risk treatment plan in place.

Minimum Security Standards

Bobcat Desktop – Let OIT do it for you!

All devices connected to UC Merced networks must meet minimum security standards, including:

- *Anti-malware software*
- *Encryption and backup/recovery software (P3 data and higher)*
- *Strong password and/or PIN lock, screen timeout*
- *Running a supported OS with security patches applied regularly*

Risk Assessment & Treatment

IS-3 requires units to conduct regular risk assessments and develop risk treatment plans

- Risk Assessments for Faculty PIs: *Research Data Security Assurance Consultation* (OIT Service Hub)
- We conduct a risk assessment of your environment with you – classify data, confirm appropriate controls
- Final Result: Risk Treatment Plan, including any documented exceptions

Wrapping Things Up

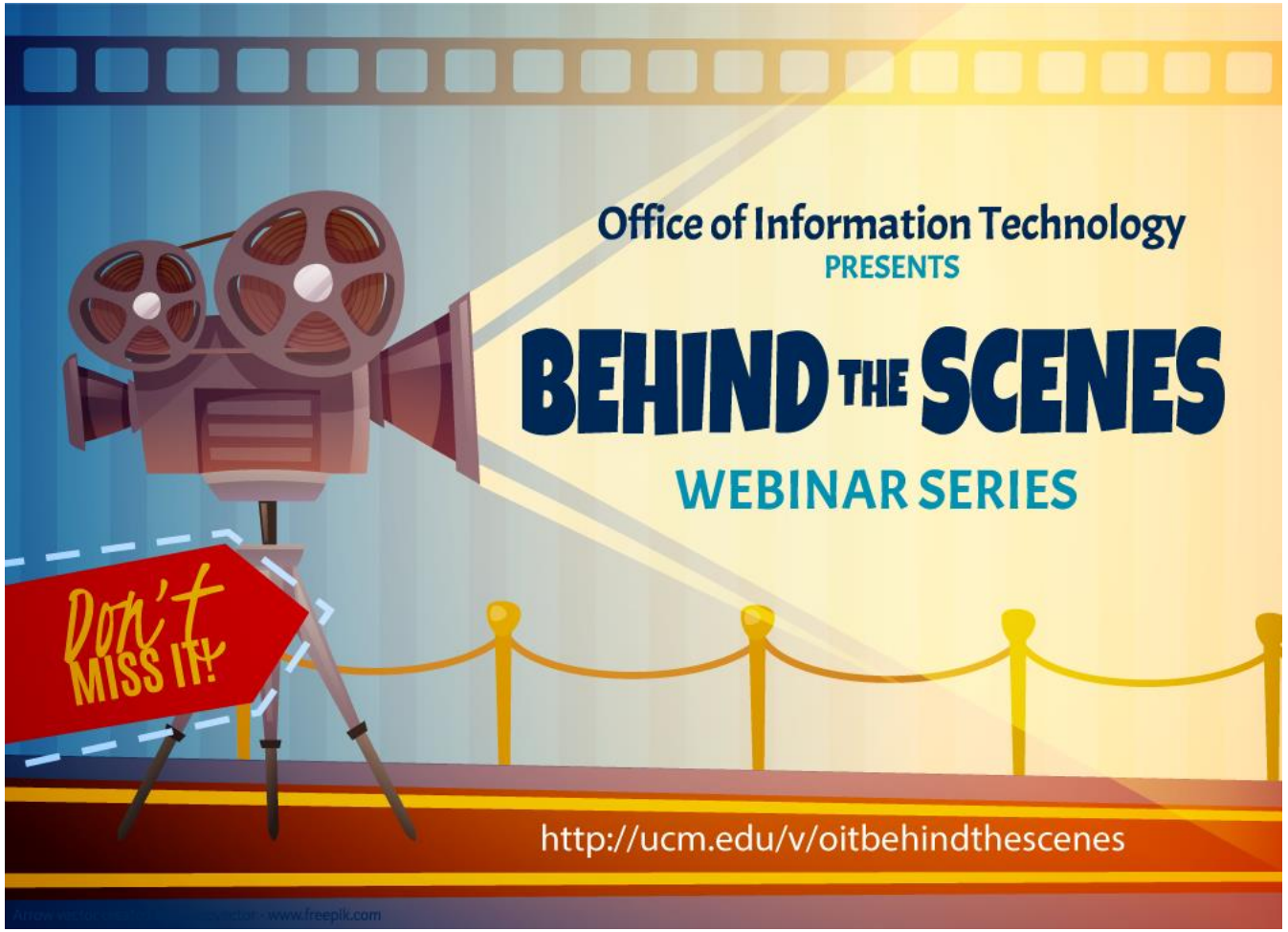
Key Points To Remember

- Security is the responsibility of all Workforce members
- P3 and P4 data have special requirements for protection
- OIT can take care of minimum security requirements for you!
- Risk Assessments and Risk Treatment plans are mandatory – OIT will be ramping up this service and consultation with Units in 2022

Ask Me Anything

COMING SOON: MORE BEHIND THE SCENES!

Summer: Microsoft365 Tools



http://ucm.edu/v/oitbehindthescenes

OIT Behind the Scenes: IS-3 Ask Me Anything was created on location at the University of California, Merced in Merced, California!

Thanks to all the OIT folks
who put hard work into this webinar!

Katie Adams Arca
Webinar Coordinator

Nicholas Dugan
Interim Chief Information Officer

Calvin Hoang
Student Technology Consultant

Edson Gonzales
Webinar Support

Preethi Merugumala
Student Technology Consultant Supervisor

Christian Ortiz

That's all, folks!