IS-3
A Next Generation Policy
UCCSC

August 2018

Robert Smith

Systemwide IT Policy Director

"As counterintuitive as it sounds, cybersecurity is a human problem, it's a leadership problem, it's not a technical problem,"

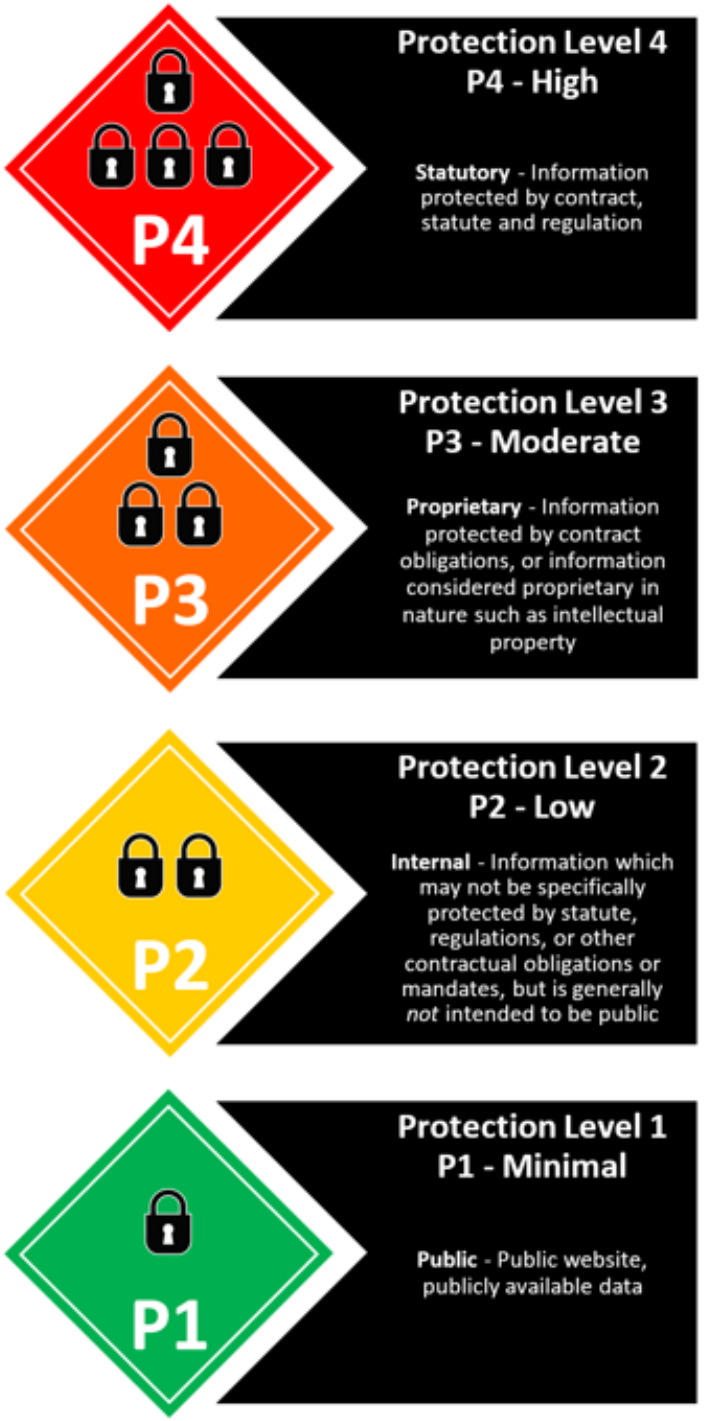
Eric Rosenbach, who leads the Defending Digital Democracy Project, a bipartisan effort devoted to election cybersecurity at Harvard Kennedy School's Belfer Center.

Replacement & Retirement

- The new IS-3
  - Replaces the current IS-3
  - Retires IS-2 (Inventory, Classification, and Release of University Electronic Information)
  - Retires IS-10 (Systems Development Standards)

Round 1

THE BASICS

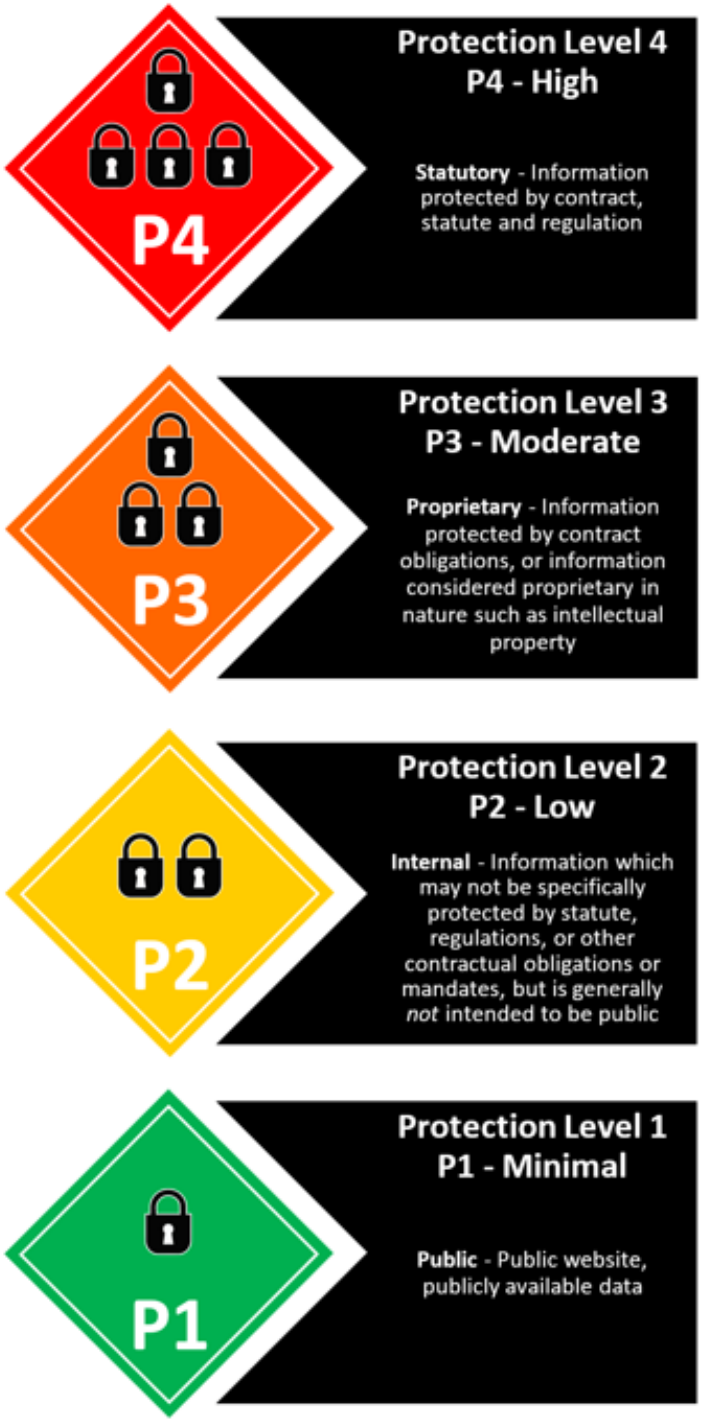


Key terms

- Location
- Unit
- Unit Head
- Unit Information Security Lead (UISL)
- Workforce Member
- Workforce Manager

Key Terms Continued

- Protection Level
  - 1 to 4
- Availability Level
  - 1 to 4
- Critical IT Infrastructure
  - Shared fate systems – require special handling



8 things to know

1. CISO is a central role
   a) Local control!
2. There is a built-in exception process (2.2)
3. 4 ways to be compliant
   a) See the next slide
4. This is a minimum security baseline
   a) Every non-lab location participated
   b) But – some situations are going to require more controls
5. Segmentation (isolation) is a premise
   a) Because it is good security
   b) PCI and NIST 800-171 say so
   c) It's practical for HIPAA compliance
   d) It's a sound defensive strategy for the future
   e) But, this does not make it an absolute
6. Critical IT Infrastructure is special
7. 4 Protection Levels and 4 Availability Levels scope controls
8. ISMP – is the bridge – old IS-3 to new
   a) This allows current work to be used in transition

4 Ways to Comply

- Perform a full Risk Assessment
  - Must use at least the IS-3 + Standard Control sets
- The pre-approved Risk Treatment Plan
  - CISO must approve
- Follow the full set of controls
  - ~365 Control sets
- Some combination of the above

Auditability

- Uses “must” language
- Uses these forms
  - Un-scoped
    - Must do x
  - Scoped
    - For > P2 then must do
    - For > A2 then must do
    - For > P2 and A2 then must do
- Risk treatment plans set specific criteria
- Risk assessment (full) trumps everything

Adoption

- Security is a technical domain
- Securty.ucop.edu will add resources to help our users
  - Locations are doing the same
    - https://security.uci.edu/
    - http://itcatalog.ucdavis.edu/category/security
  - This is a common need across research universities
    - How do we make good security a habit?

Guide Posts

6 Goals

- Preserve academic and research collaboration
- Protect privacy
- Follow a risk-based approach
- Maintain confidentiality
- Protect integrity
- Ensure availability

5 Principles

- A goal-based approach is best
- Units are accountable for implementing information security
- Decision-making rights correspond to risk level
- Security is a shared responsibility
- Security is embedded into the entire lifecycle

Cyber insurance

- IS-3 1.2.2 and BUS-80 are connected

1.2.2 Costs of an Information Security Incident

Units may bear some or all of UC's direct costs that result from an Information Security Incident under the Unit's area of responsibility if the Information Security Incident resulted from a significant failure of the Unit to comply with this policy. These costs include, but are not limited to: the response, containment, remediation, forensics, analysis, notification, litigation, penalties, regulatory fines and any other costs directly attributable to the Information Security Incident.

A significant failure to comply may affect the Unit's or the Location's ability to seek cyber insurance reimbursement under Business and Finance Bulletin BUS-80 - Insurance Programs for Information Technology Systems.

Round 2

POLICY STRUCTURE

Scope

- Covers “Workforce Members”
  - Employee, faculty, staff, contractor, student worker
  - Volunteer, student intern, student volunteer
  - Researcher, student supporting/performing research
  - Medical center staff/personnel, clinician
  - Medical school student treating patients
  - Person working for UC in any capacity or other augmentation to UC staffing levels
- Covers Suppliers
- Students simply attending the university are not in scope!

Part III Outline

1. General Overview
2. Organizing Information Security
3. Roles and Responsibilities
4. Information Security Management Program Principles
5. Information Security Management Program
6. Risk Management Process
7. Human Resource Security
8. Asset Management
9. Subsections 9 – 18 are the technical controls

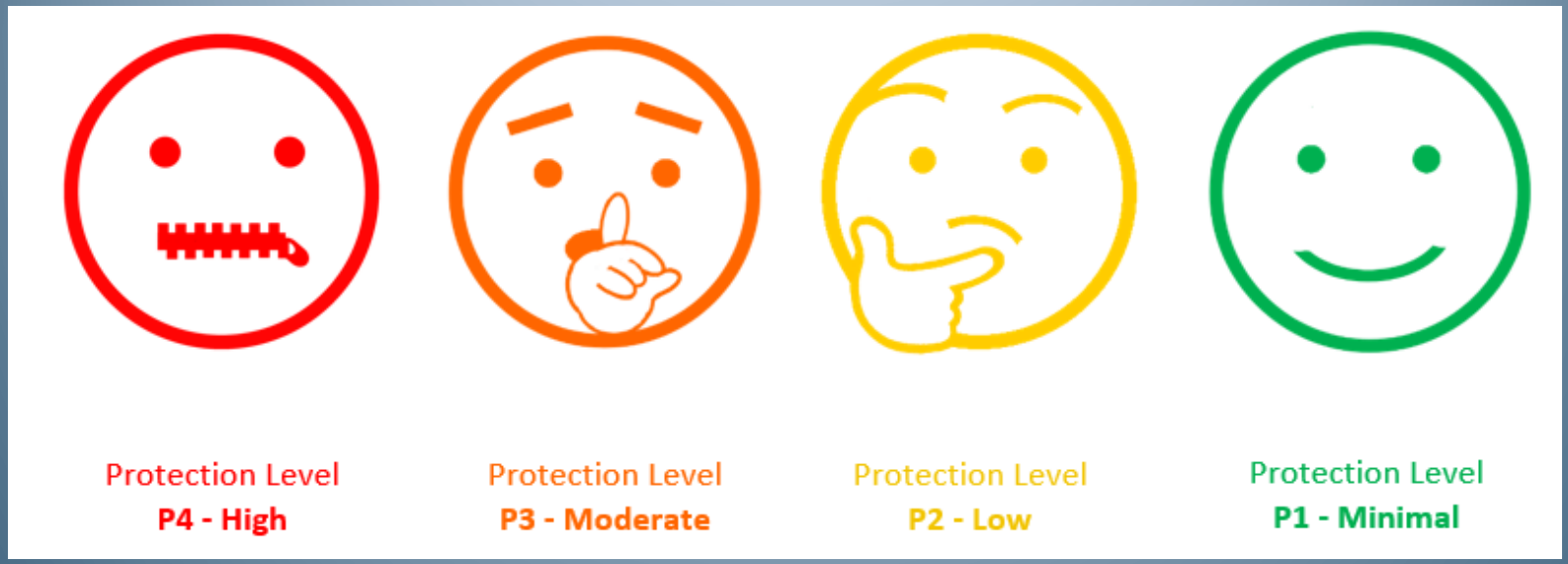
Follows the ISO 27002 Outline

- Sections 7 to 18 follow ISO 27002 to the x.x level
- Benefits
  - Cyber insurance
  - Ties to all major crosswalks
  - Ties to off-the-shelf software
  - Ties to vendor services
  - Significant ecosystem that explains what each control means
- IS-3 puts a control on the “one best place”
- UC picked the best subset of controls for a public research university

9 Standards

1. UC Authentication Management Standard
2. UC Data Destruction Standard
3. UC Encryption Key and Certificate Management Standard
4. UC Institutional Information and IT Resource Classification Standard
5. UC Logging and Event Recording Standard
6. UC Minimum Security Standard
7. UC Secure Software Configuration Standard
8. UC Privacy and Data Security Incident Response Plan Standard
9. UC Secure Software Development Standard

https://security.ucop.edu/policies/index.html



Round 4

PROTECTION AND AVAILABILITY LEVELS

Protection and Availability Levels

- Protection Level
  - Follows the “Institutional Information”
- Availability Level
  - Follows the “Institutional Information”
- Both are used for IT Resources, too
- Scopes controls

Protection Level	
P1	Public information or information intended to be readily obtainable by the public, but whose integrity is important and for which unauthorized modification is the primary protection concern. IT Resources where the application of minimum security requirements is sufficient
P2	May not be specifically protected by statute, regulations or other contractual obligations or mandates, but are generally not intended for public use or access
P3	Unauthorized disclosure or modification could result in small to moderate fines, penalties or civil actions. Could result in moderate damage to UC, its students, patients, research subjects, employees, community and/or reputation; could have a moderate impact on the privacy of a group; could result in moderate financial loss
P4	Statutory, regulatory and contract obligations are major drivers for this risk level. Other drivers include, but are not limited to, the risk of significant harm or impairment to UC students, patients, research subjects, employees, guests/program participants, UC reputation, the overall operation of the Location or essential services

Availability Level	
A1	Loss of availability poses minimal impact or financial losses
A2	Loss of availability may cause minor losses or inefficiencies
A3	Loss of availability would result in moderate financial losses and/or reduced customer service
A4	Loss of availability would result in major impairment to the overall operation of the Location and/or essential services, and/or cause significant financial losses. IT Resources that are required by statutory, regulatory and legal obligations are major drivers for this risk level

Round 3

KEY FEATURES

Key Features

- Security is a shared responsibility
  - Everyone has a role
  - This drove our fundamental approach
- Units as a point of accountability
  - Unit Heads
    - Dean, VC, AVC, Provost, Executive Director
  - Unit Information Security Leads – liaison
    - CISO needs to support this role

Key Features (continued)

- Basic Coverage for:
  - HIPAA + HITECH
  - PCI 3.2
  - NIST 800-171
  - GLBA
  - NIST CSF
- Scalable
  - Pre-approved risk treatment plan
  - Yes – it's a check list, but …
  - The policy is risked-based
    - So UC wants the resources applied where the risk is

Key Features (continued)

- Built in exception process (2.2)
  - Location CISO approves
  - Specific requirements
- Information Security Management Program
  - Location requirement
  - Bridges old policy approach to the new one
  - Get's Location started more or less on day 0

Key Features (continued)

- Directly implementable
  - Contains specific requirements – Units "must"
  - Common UC policy across the system
  - Non-health Locations should not "need" additional Policies for general information security
    - Procedures may be required
- Risk management
  - Aligned with NIST CSF and NIST 800-39
  - Made this a simple(r) topic

Key Features (continued)

- Researcher/Principal Investigator called out
  - Specific requirements – allows **them to be in control**. This was the top request from PIs.
  - 4 options for PIs:
    - Use a Service Provider
    - Use a (Pre-approved) Risk Treatment Plan
    - Build their own plan using a risk assessment or the full control set
    - Or some combination

Round 5

ROLES IN OUR APPROACH

[Unique] Roles

- CISO
  - Rock star of the policy
- Unit Head
  - Dean, VC, AVC, Provost, Executive Director
  - Principal Investigator in some cases
- Unit Information Security Lead
  - A role focused on compliance – risk management
  - CISO must have a program to support this role
    - Important to scale out the program
- CRE
  - The top risk manager, controls budget and risk tolerance for the Location

[Unique] Roles (continued)

- Service Provider
  - Delivers information technology services that comply with this policy.
  - Documents and delivers IT services in compliance with this policy, other UC policies and applicable Location policies.
  - Notifies the Unit Head of any policy provisions that are unmet or that require additional controls by the Unit.

Expected Roles

- Chancellors
- Cyber-risk Responsible Executive (CRE)
- CISO
- UC Systemwide Chief Information Security Officer
- CIO
- Institutional Information Proprietor
- IT Resource Proprietor
- Workforce Manager
- Workforce Member
- PI/Researcher

Summary

- 4 ways to comply
- Risk based
- Local control
- Flexible and scalable
  - Risk Treatment Plans
- Units and Unit Heads are responsible!
- Tailored catalog of requirements for UC
- Location controlled exception process
- Designed to manage risk
- Encourages Units and CISO to “have the conversation”
- Ties to cyber insurance coverage

Thank You!

Questions

Other resources

- My Contact Information
  - Robert.smith@ucop.edu
  - 510-587-6244
- Supporting website is live https://security.ucop.edu/policies/index.html