

UC Electronic Information Security (IS-3) Program Assessment

http://www.ucop.edu/uccophome/policies/bfb/is3.pdf

A	B	C	D	H	I	J
	Current Maturity Level (Baseline)	Planned Maturity / Goal for 2007-08	Campus (excluding Central/Campus-wide IT) Describe status/evolution - include brief detail, such as breadth, maturity, and percentage estimates for the campus overall, excluding Central/Campus-wide IT.			
1						
2	IS - 3 Policy Requirements	0 - Not Performed 1 - Performed Informally 2 - Planned and Tracked 3 - Well Defined and Communicated 4 - Managed and Measurable 5 - Continuously Improving				
3						
4	Security Program					
5	Identification of Information Security Officer (III.A)	2	2	Most units have identified individuals solely or partly responsible for security.		
6	Designate an individual to perform the function of an Information Security Officer(s) on each campus.					
7	Security Plan (III.C)					
8	Define/update the "security objectives" for confidentiality, integrity, and availability of information resources, describing the potential harm/security impact that failure to achieve security objectives would have on the operations, function, image/reputation, or ability to protect personal information.	2	2	Most units have identified data and actively protect the data. However, these standards and procedures vary from unit to unit and most units rely more on the knowledge of individuals as opposed to documented standards.		
9	Education & Security Awareness Training (III.E)					
10	Conduct appropriate security awareness training for faculty, staff, and students.	1	2	Training in units varies greatly and is often informal or non-existent.		
11	Identity and Access Management					
12	Control access by authentication and authorization mechanisms to insure that only identifiable individuals with appropriate authorization gain access to specified computing and information resources. (Identity and Access Management (III.C.2.a))	2	2	Units take measures to ensure appropriate access to sensitive data. These schemes vary from unit to unit and are not standardized except for informal sharing.		
13	Security Program Processes					
14	Risk Assessment, Asset Inventory & Classification (III.B)					
15	Inventory computing devices (servers, desktop computers, laptops, mobile devices, storage devices, etc.) and the characteristics of the information/data stored on or transmitted from/to those computing devices. Inventory applications and the characteristics of the data stored by or transmitted from/to those applications.	1	1	Most units have an understanding of the data they hold which ranges from informal to formal. In most cases, aside from identifying sensitive information, the data is not formally classified and documented.		
16	Classify each computing device and application based on the characteristics of the associated stored data or data transmitted from/to the computing device or application.					
17	Workforce/Administrative (III.C.1)					
18	Control how faculty, staff, students, and other affiliates are granted access privileges to computing and information resources and how those privileges for individuals are altered or revoked. Review privileged account access.	3	3	Personnel are appropriately screened. Units take efforts to maintain proper access to different levels and the differences of access to resources to varying groups, such as faculty and students, is understood.		
19	Conduct appropriate background checks for personnel handling information classified as "sensitive" or "to be protected."					
20	Take appropriate personnel/disciplinary action(s) for violations of policy/procedures.					
21	Applications Systems Management					

UC Electronic Information Security (IS-3) Program Assessment

http://www.ucop.edu/ucophome/policies/bfb/is3.pdf

	A	B	C	D	H	I	J
		Current Maturity Level (Baseline)	Planned Maturity/Goal for 2007-08	Campus (excluding Central/Campus-wide IT)			
1				Describe status/action - include brief detail, such as breadth, maturity, and percentage estimates for the campus overall, excluding Central/Campus-wide IT.			
2	IS - 3 Policy Requirements	0 - Not Performed 1 - Performed Informally 2 - Planned and Tracked 3 - Well Defined and Communicated 4 - Managed and Measurable 5 - Continuously Improving					
3	<ul style="list-style-type: none"> Control application systems development/maintenance through conformance with specifications in IS-10, local standards, procedures, guidelines, and conventions; conduct application vulnerability assessments as appropriate. [System & Applications Software Development (III.C.2.c.v)] Control production application software modification through change management procedures for major systems. - [Change Management (III.C.2.e)] 	1	1	Development life cycles vary on the resources of the units. The web developers group is meeting on a regular basis to help define better standards. Change management practices need to be better outlined.			
19	Risk Mitigation Measures (III.C.3.a)						
20	Protect resources in the event of emergencies.			[TBD]			
21	Incident Response Planning & Notification Procedures (III.D)						
22	Maintain incident response and notification processes.	3	3	Most units do not have formal incident response plans in place, but key individuals understand how to handle a situation and Central Guidelines are published.			
23	Third Party Agreements (III.F)						
24	Ensure that contracts with external entities include data security language.			[TBD]			
25	Security Controls						
26	Access Controls (III.C.2.b)						
27	Control passwords and sessions to minimize risk of unauthorized access to restricted computing and information resources: <ul style="list-style-type: none"> Control passwords through password management conventions and vulnerability assessment procedures. - [Passwords and other authentication credentials (III.C.2.b.i)] Control access to working sessions through session timeout mechanisms. - [Session protection (III.C.2.b.ii)] Control privileged account access through defined procedures for providing privileged accounts and reviewing activity under privileged account. - [Privileged access (III.C.2.b.iii)] 	2	3	For web applications and some server access, units rely on the centralized authentication system. For those who do not, access schemes vary widely. Reviewing provisioned access does not happen as often as it should.			
28	Systems and Application Security (III.C.2.c)						
29	Control systems-level access through review of personnel assignments for appropriate classification, security responsibilities, and separation of duties. [Systems Personnel (III.C.2.c.i)] <ul style="list-style-type: none"> Backup systems supporting essential activities; encrypt data where required to secure backup data. - [Back Up and Retention (III.C.2.c.ii)] Protect computing and information resources from malicious software (e.g., viruses, worms, Trojans, spyware, etc.) - [System Protection (III.C.2.c.iii)] Maintain currency of operating systems and application systems software. - [Patch Management (III.C.2.c.iv)] 	4	4	Units are effective in managing malware and maintain current patch levels. Mobile users present difficulties to this. Backups are common. Personnel is general well reviewed, though resource strain often prevents a complete separation of duties.			
30							

UC Electronic Information Security (IS-3) Program Assessment

http://www.ucop.edu/ucohome/policies/bfbi/is3.pdf

A	B	C	D	H	I	J
			Campus (excluding Central/Campus-wide IT)			
	Current Maturity / Level (Baseline)	Planned Maturity / Goal for 2007-08	Describe status/action - include brief detail, such as breadth, maturity, and percentage estimates for the campus overall, excluding Central/Campus-wide IT.			
1						
2						
3						
31	1	1				
32						
33	3	3				
34						
35	3	3				
36						
37						

UC Electronic Information Security (IS-3) Program Assessment

http://www.ucop.edu/ucophome/policies/bf/bf/is3.pdf

	A	B	C	D	H	I	J
		Campus (excluding Central/Campus-wide IT)					
		Current Maturity Level (Baseline)	Planned Maturity / Goal for 2007-08	Describe status/action - Include brief detail, such as breadth, maturity, and percentage estimates for the campus overall, excluding Central/Campus-wide IT.			
1							
2	IS - 3 Policy Requirements						
3	Control network and computing resources exposure to risk through minimum network connectivity requirements, firewalls and Intrusion Detection System/Intrusion Prevention System (IDS/IPS) as appropriate: <ul style="list-style-type: none"> • Control access to networked devices through authentication measures (e.g. user name/password or better). - [Access Control Measures (I.V.A.)] • Protect passwords or other authentication tokens while in transit through the use of encryption. - [Encrypted Authentication (I.V.B.)] • Control potential security loopholes by maintaining current operating system, application software, and firmware code on all devices connected to the network. - [Patch Management Practices (I.V.C.)] • Protect networked devices against malicious software. - [Malicious Software Protection (I.V.D.)] • Control the use of networked devices for intended purposes by eliminating unnecessary services from devices. - [Removal of Unnecessary Services (I.V.E.)] • Control network communications to/from networked devices through host-based firewall software, as available. - [Host-based Firewall Software (I.V.F.)] • Prevent networked devices from becoming unauthorized email relays. - [Authenticated Email Relay (I.V.G.)] • Control access to network proxy servers through authentication [Authenticated Network Proxy Servers (I.V.H.)] • Control access to restricted or essential services by limiting unattended/inactive sessions through session timeouts. - [Session Timeout (I.V.I)] 	0 - Not Performed 1 - Performed Informally 2 - Planned and Tracked 3 - Well Defined and Communicated 4 - Managed and Measurable 5 - Continuously Improving					
38				Most units practice effective practices which conform to the minimum requirements. Problems often relate to individuals or groups which opt out of standardized support. In general, systems are maintained, with proper patch levels, appropriate services, and anti-virus. These standards are well communicated and well accepted.			
39							
40							
41							
43							
45							

0 Not performed—Complete lack of any recognizable processes. The institution has not even recognized that there is an issue to be addressed.

1 Performed Informally—there is evidence that the institution has recognized that the issues exist and need to be addressed. There are, however, no standardized processes; instead, there are ad hoc approaches that tend to be applied on an individual or case-by-case basis. The overall approach to management is disorganized.

2 Planned and Tracked—Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely.

UC Electronic Information Security (IS-3) Program Assessment

<http://www.ucop.edu/ucohome/policies/bfb/is3.pdf>

	A	B	C	D	H	I	J
1							
2	<p>IS - 3 Policy Requirements</p>	<p>Current Maturity Level (Baseline)</p> <p>0 - Not Performed 1 - Performed Informally 2 - Planned and Tracked 3 - Well Defined and Communicated 4 - Managed and Measurable 5 - Continuously Improving</p>	<p>Planned Maturity / Goal for 2007-08</p>	<p>Campus (excluding Central/Campus-wide IT)</p> <p>Describe status/action - include brief detail, such as breadth, maturity, and percentage estimates for the campus overall, excluding Central/Campus-wide IT.</p>			
3							
47	<p>3 Well Defined and Communicated —Procedures have been standardized and documented, and communicated through training. It is mandated that these processes should be followed; however, it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalization of existing practices.</p>						
49	<p>4 Managed and Measurable—Management monitors and measures compliance with procedures and takes action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.</p>						
51	<p>5 Continuously Improved —Processes have been refined to a level of good practice, based on the results of continuous improvement and maturity modeling with other enterprises. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.</p>						

