

UC Electronic Information Security (IS-3) Program Assessment

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

	A	B	C	D	E	F	G	H	I	J
1		Central/Campus-wide IT			Campus (excluding Central/Campus-wide IT)			Medical Centers		
2	IS - 3 Policy Requirements	Current Maturity Level (Baseline)	Planned Maturity / Goal for 2007-08	Describe status/action - include brief detail, such as breadth, maturity, and percentage estimates for 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.	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 affiliated medical center.
3		0 - Not Performed 1 - Performed Informally 2 - Planned and Tracked 3 - Well Defined and Communicated 4 - Managed and Measurable 5 - Continuously Improving			0 - Not Performed 1 - Performed Informally 2 - Planned and Tracked 3 - Well Defined and Communicated 4 - Managed and Measurable 5 - Continuously Improving			0 - Not Performed 1 - Performed Informally 2 - Planned and Tracked 3 - Well Defined and Communicated 4 - Managed and Measurable 5 - Continuously Improving		
4	Security Program									
5	Identification of Information Security Officer (III.A)									
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.									
9	Education & Security Awareness Training (III.E)									
10	Conduct appropriate security awareness training for faculty, staff, and students.									
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)]									
13	Security Program Processes									
14	Risk Assessment, Asset Inventory & Classification (III.B)									
15	<ul style="list-style-type: none"> • 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. • 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. 									
16	[Workforce] Administrative (III.C.1)									

UC Electronic Information Security (IS-3) Program Assessment

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

	A	B	C	D	E	F	G	H	I	J
1		Central/Campus-wide IT			Campus (excluding Central/Campus-wide IT)			Medical Centers		
2	IS - 3 Policy Requirements	Current Maturity Level (Baseline)	Planned Maturity / Goal for 2007-08	Describe status/action - include brief detail, such as breadth, maturity, and percentage estimates for 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.	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 affiliated medical center.
3		0 - Not Performed 1 - Performed Informally 2 - Planned and Tracked 3 - Well Defined and Communicated 4 - Managed and Measurable 5 - Continuously Improving			0 - Not Performed 1 - Performed Informally 2 - Planned and Tracked 3 - Well Defined and Communicated 4 - Managed and Measurable 5 - Continuously Improving			0 - Not Performed 1 - Performed Informally 2 - Planned and Tracked 3 - Well Defined and Communicated 4 - Managed and Measurable 5 - Continuously Improving		
17	<ul style="list-style-type: none"> 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. Conduct appropriate background checks for personnel handling information classified as "sensitive" or "to be protected." Take appropriate personnel/disciplinary action(s) for violations of policy/procedures. 									
18	Applications Systems Management									
19	<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)] 									
20	Risk Mitigation Measures (III.C.3.a)									
21	Protect resources in the event of emergencies.									
22	Incident Response Planning & Notification Procedures (III.D)									
23	Maintain incident response and notification processes.									
24	Third Party Agreements (III.F)									
25	Ensure that contracts with external entities include data security language.									
26	Security Controls									
27	Access Controls (III.C.2.b)									
28	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)] 									

UC Electronic Information Security (IS-3) Program Assessment

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

	A	B	C	D	E	F	G	H	I	J
1		Central/Campus-wide IT			Campus (excluding Central/Campus-wide IT)			Medical Centers		
2	IS - 3 Policy Requirements	Current Maturity Level (Baseline)	Planned Maturity / Goal for 2007-08	Describe status/action - include brief detail, such as breadth, maturity, and percentage estimates for 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.	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 affiliated medical center.
3		0 - Not Performed 1 - Performed Informally 2 - Planned and Tracked 3 - Well Defined and Communicated 4 - Managed and Measurable 5 - Continuously Improving			0 - Not Performed 1 - Performed Informally 2 - Planned and Tracked 3 - Well Defined and Communicated 4 - Managed and Measurable 5 - Continuously Improving			0 - Not Performed 1 - Performed Informally 2 - Planned and Tracked 3 - Well Defined and Communicated 4 - Managed and Measurable 5 - Continuously Improving		
29	Systems and Application Security (III.C.2.c)									
30	<ul style="list-style-type: none"> • 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)] • 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)] 									
31	Audit Logs (III.C.2.f)									
32	Monitor for attempted/actual unauthorized access through review of access and audit logs.									
33	Encryption (III.C.2.g)									
34	Control risk of unauthorized access to "sensitive"/"restricted" data by use of encryption.									
35	Physical/Environmental Controls (III.C.3)									
36	<ul style="list-style-type: none"> • Control access to facilities by appropriate measures - [Physical Access Controls (III.C.3.b)] • Track movement of devices - [Tracking Reassignment or Movement of Devices & Stock Inventories (III.C.3.c)] • Remove data before equipment is re-deployed, recycled, or disposed. - [Disposition of Equipment (III.C.3.d)] • Control physical security of portable media. - [Portable & Media Devices (III.C.3.e)] 									
37	Network Security (III.C.2.d) / Minimum Requirements for Network Connectivity (IV)									

UC Electronic Information Security (IS-3) Program Assessment

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

	A	B	C	D	E	F	G	H	I	J
1		Central/Campus-wide IT			Campus (excluding Central/Campus-wide IT)			Medical Centers		
2	IS - 3 Policy Requirements	Current Maturity Level (Baseline)	Planned Maturity / Goal for 2007-08	Describe status/action - include brief detail, such as breadth, maturity, and percentage estimates for 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.	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 affiliated medical center.
3		0 - Not Performed 1 - Performed Informally 2 - Planned and Tracked 3 - Well Defined and Communicated 4 - Managed and Measurable 5 - Continuously Improving			0 - Not Performed 1 - Performed Informally 2 - Planned and Tracked 3 - Well Defined and Communicated 4 - Managed and Measurable 5 - Continuously Improving			0 - Not Performed 1 - Performed Informally 2 - Planned and Tracked 3 - Well Defined and Communicated 4 - Managed and Measurable 5 - Continuously Improving		
38	<p>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:</p> <ul style="list-style-type: none"> • Control access to networked devices through authentication measures (e.g. user name/password or better). - [Access Control Measures (IV.A.)] • Protect passwords or other authentication tokens while in transit through the use of encryption. - [Encrypted Authentication (IV.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 (IV.C.)] • Protect networked devices against malicious software. - [Malicious Software Protection (IV.D.)] • Control the use of networked devices for intended purposes by eliminating unnecessary services from devices. - [Removal of Unnecessary Services (IV.E.)] • Control network communications to/from networked devices through host-based firewall software, as available. - [Host-based Firewall Software (IV.F.)] • Prevent networked devices from becoming unauthorized email relays. - [Authenticated Email Relay (IV.G.)] • Control access to network proxy servers through authentication [Authenticated Network Proxy Servers (IV.H.)] • Control access to restricted or essential services by limiting unattended/inactive sessions through session timeouts. - [Session Timeout (IV.I.)] 									
39										
40	Definitions									
41	0 Not performed —Complete lack of any recognizable processes. The institution has not even recognized that there is an issue to be addressed.									
43	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.									

UC Electronic Information Security (IS-3) Program Assessment

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

	A	B	C	D	E	F	G	H	I	J
1		Central/Campus-wide IT			Campus (excluding Central/Campus-wide IT)			Medical Centers		
2	IS - 3 Policy Requirements	Current Maturity Level (Baseline)	Planned Maturity / Goal for 2007-08	Describe status/action - include brief detail, such as breadth, maturity, and percentage estimates for 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.	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 affiliated medical center.
3		0 - Not Performed 1 - Performed Informally 2 - Planned and Tracked 3 - Well Defined and Communicated 4 - Managed and Measurable 5 - Continuously Improving			0 - Not Performed 1 - Performed Informally 2 - Planned and Tracked 3 - Well Defined and Communicated 4 - Managed and Measurable 5 - Continuously Improving			0 - Not Performed 1 - Performed Informally 2 - Planned and Tracked 3 - Well Defined and Communicated 4 - Managed and Measurable 5 - Continuously Improving		
45	<p>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.</p>									
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>									