Section	Topic Responsible (R), Accountable (A), Consulted (C), Informed (I)	Employee	HR Liaison	Org Unit Head	Developer	IT Service Provider	Campus ISO	Campus CIO
1.1	**Access Control**							
1.1.1	AC-2 Account Management Additional Controls					A		
1.1.2	AC-6 Least Privilege					R		
1.1.3	AC-11 Session Lock						A	
1.1.4	AC-17 Remote Access						R	
1.1.5	AC-19 Access Control for Mobile Devices					A	R/C	
1.1.6	AC-20 Use of External Information Systems					A	R/C	
1.2	**Awareness and Training**							
1.2.1	AT-2 Security Awareness	R		A				
1.3	**Audit and Accountability**							
1.3.1	AU-2 Audit Events					A	C	
1.3.2	AU-2 Content of Audit Records					A	C	
1.3.3	AU-6 Audit Review, Analysis, and Reporting					A	C	
1.3.4	AU-8 Time Stamps					A	C	
1.3.5	AU-9 Protection of Audit Records					A	C	
1.3.6	AU-10 Non-Repudiation					R	R/C	
1.3.7	AU-12 Audit Generation					A	A	
1.4	**Security Assessment and Authorization**							
1.4.1	CA-2Security Assessment						A	
1.4.2	CA-8 Penetration Testing					C	A	
1.4.3	CA-7 Continuous Monitoring					A	C	
1.5	**Configuration Management**							
1.5.1	CM-2 Baseline Configuration						A	
1.5.2	CM-3 Configuration Change Control					A		
1.5.3	CM-5 Access Restrictions for Change					A		
1.5.4	CM-6 Configuration Settings					A		
1.5.5	CM-7 Least Functionality					A		
1.5.6	CM-8 Information System Component Inventory					A		
1.6	**Contingency Planning**							
1.6.1	CP-2 Contingency Plan					A	C	
1.6.2	CP-4 Contingency Plan Testing					A	C	
1.6.3	CP-6 Alternate Storage Site					A		
1.6.4	CP-7 Alternate Processing Site					A		
1.6.5	CP-8 Telecommunications Services							A
1.6.6	CP-10 Information System Recovery					A		
1.7	**Identification and Authentication**							
1.7.1	IA-2 User Identification and Authentication					A	C	
1.8	**Incident Response**							
1.8.1	IR-4 Incident Handling						A	
1.8.2	IR-5 Incident Monitoring					A	C	
1.8.3	IR-6 Incident Reporting					A	C	
1.9	**Maintenance**							
1.9.1	MA-4 Non-Local Maintenance					A	I	
1.10	**Media Protection**							
1.10.1	MP-4 Media Transport					A		
1.10.2	MP-7 Media Use	R				R	R/C	A
1.11	**Physical and Environmental Protection**							
1.11.1	PE-13 Location of Information System Components			A			C	
1.12	**Planning**							
1.12.1	PL-2 System Security Plan					C	A	
1.13	**Personnel Security**							
1.13.1	PS-4 Personnel Termination		A			A	R	
1.14	**Risk Assessment**							
1.14.1	RA-5 Vulnerability Scanning						A	
1.15	**System and Services Acquisition**							
1.15.1	SA-4 Acquisitions					A		
1.15.2	SA-15 Development Process, Standards, and Tools				R	A	C	
1.15.3	SA-17 Developer Security Architecture and Design				R	A	C	
1.16	**System and Communications Protection**							
1.16.1	SC-7 Boundary Protection					R		A
1.16.2	SC-8 Transmission Confidentiality					A		
1.17	**System and Information Integrity**							
1.17.1	SI-3 Malicious Code Protection					R	C	A
1.17.2	SI-4 Information System Monitoring					A	C	
1.17.3	SI-7 Software, Firmware, and Information Integrity					A	C	