INFORMATION SYSTEMS

In November 2011, The University of North Carolina Information Technology Security Council [ITSC] recommended the adoption of ISO/IEC 27002 Information technology - Security techniques - Code of practice for information security management [ISO 27002] as the common security framework baseline to be used by the campuses of the University of North Carolina system to develop their individual institutional information technology security policies. The referenced implementation standards are the NC IT Security Manual, the Control Objectives for Information and related Technology (COBIT), and the National Institute of Standards and Technology (NIST). These standards are recognized nationally and within NC by the NC Office of State Auditors and the NC Office of the CIO. The ITSC will also supplement this crosswalk table with specific UNC campus implementation examples as those are made available to the ITSC by the campus security officer. Each campus is strongly encouraged to consider these implementation standards when developing their specific IT security policies.

At UNC Charlotte, these standards apply to all software and hardware systems. ITS is accountable for meeting the established standards for software and hardware under ITS control. Departments, colleges and divisions that independently manage software and hardware outside ITS control are accountable to meet the same standards as ITS.

Applicable external policies or procedures:

- ISO/IEC 27002 Information Technology - Security Techniques

University policies or procedures:

- University Policy 302: Web Communications
- University Policy 303: Network Security
- University Policy 304: Electronic Communication Systems
- University Policy 307: Responsible Use of University Computing and Electronic Communication Resources
- University Policy 311: Information Security and all supplemental regulations, standards, and guidelines
- University Policy 315: Copyright Policy
- University Policy 317: Mobile Communication Devices
- Policy Statement # 601.14, Proprietary Software

ISO 27002 Chapter	Section	Control	Applicable to unit?	Current Condition?	Meets Standard?	Remediation Required?	Risk Level
05.0 Security Policy	05.01 Information security policy	05.01.01 Information security policy document					
		05.01.02 Review of the information security policy					
07.0 Asset Management	07.01 Responsibility for assets	07.01.01 Inventory of assets					
		07.01.02 Ownership of assets					
		07.01.03 Acceptable use of assets					
	07.02 Information classification	07.02.01 Classification guidelines					
		07.02.02 Information labeling and handling					
08.0 Human Resource Security	08.01 Prior to employment	08.01.01 Roles and responsibilities					
		08.01.02 Screening					
		08.01.03 Terms and conditions of employment					
	08.02 During employment	08.02.01 Management responsibilities					
		08.02.02 Information security awareness, education, and training					
		08.02.03 Disciplinary process					
	08.03 Termination or change of employment	08.03.01 Termination responsibilities					
		08.03.02 Return of assets					
		08.03.03 Removal of access rights					
09.0 Physical and Environmental Security	09.01 Secure areas	09.01.01 Physical security perimeter					
		09.01.02 Physical entry controls					
		09.01.03 Securing offices, rooms, and facilities					
		09.01.04 Protecting against external and environmental threats					
		09.01.05 Working in secure areas					
		09.01.06 Public access, delivery, and loading areas					
	09.02 Equipment security	09.02.01 Equipment siting and protection					
		09.02.02 Supporting utilities					
		09.02.03 Cabling security					
		09.02.04 Equipment maintenance					
		09.02.05 Security of equipment off-premises					
		09.02.06 Secure disposal or re-use of equipment					
		09.02.07 Removal of property					
10.0 Communications and Operations Management	10.01 Operational procedures and responsibilities	10.01.01 Documented operating procedures					
		10.01.02 Change management					
		10.01.03 Segregation of duties					
		10.01.04 Separation of development, test, and operational facilities					
	10.02 Third party service delivery management	10.02.01 Service delivery					
		10.02.02 Monitoring and review of third party services					
		10.02.03 Managing changes to third party services					
	10.03 System planning and acceptance	10.03.01 Capacity management					
		10.03.02 System acceptance					
	10.04 Protection against	10.04.01 Controls against malicious code					

ISO 27002 Chapter	Section	Control	Applicable to unit?	Current Condition?	Meets Standard?	Remediation Required?	Risk Level
	malicious and mobile code	10.04.02 Controls against mobile code					
	10.05 Back-up	10.05.01 Information back-up					
	10.06 Network security management	10.06.01 Network controls					
		10.06.02 Security of network services					
	10.07 Media handling	10.07.01 Management of removable media					
		10.07.02 Disposal of media					
		10.07.03 Information handling procedures					
		10.07.04 Security of system documentation					
	10.08 Exchange of information	10.08.01 Information exchange policies and procedures					
		10.08.02 Exchange agreements					
		10.08.03 Physical media in transit					
		10.08.04 Electronic messaging					
		10.08.05 Business information systems					
	10.09 Electronic commerce services	10.09.01 Electronic commerce					
		10.09.02 On-Line Transactions					
		10.09.03 Publicly available information					
	10.10 Monitoring	10.10.01 Audit logging					
		10.10.02 Monitoring system use					
		10.10.03 Protection of log information					
		10.10.04 Administrator and operator logs					
		10.10.05 Fault logging					
		10.10.06 Clock synchronization					
11.0 Access Control	11.01 Business requirement for access control	11.01.01 Access control policy					
	11.02 User access management	11.02.01 User registration					
		11.02.02 Privilege management					
		11.02.03 User password management					
		11.02.04 Review of user access rights					
	11.03 User responsibilities	11.03.01 Password use					
		11.03.02 Unattended user equipment					
		11.03.03 Clear desk and clear screen policy					
	11.04 Network access control	11.04.01 Policy on use of network services					
		11.04.02 User authentication for external connections					
		11.04.03 Equipment identification in networks					
		11.04.04 Remote diagnostic and configuration port protection					
		11.04.05 Segregation in networks					
		11.04.06 Network connection control					
		11.04.07 Network routing control					
	11.05 Operating system access control	11.05.01 Secure log-on procedures					
		11.05.02 User identification and authentication					
		11.05.03 Password management system					
		11.05.04 Use of system utilities					
		11.05.05 Session time-out					
		11.05.06 Limitation of connection time					
	11.06 Application and information access control	11.06.01 Information access restriction					
		11.06.02 Sensitive system isolation					

ISO 27002 Chapter	Section	Control	Applicable to unit?	Current Condition?	Meets Standard?	Remediation Required?	Risk Level
	11.07 Mobile computing and teleworking	11.07.01 Mobile computing and communications					
		11.07.02 Teleworking					
12.0 Information Systems Acquisition, Development and Maintenance	12.01 Security requirements of information systems	12.01.01 Security requirements analysis and specification					
	12.02 Correct processing in applications	12.02.01 Input data validation					
		12.02.02 Control of internal processing					
		12.02.03 Message integrity					
		12.02.04 Output data validation					
	12.03 Cryptographic controls	12.03.01 Policy on the use of cryptographic controls					
		12.03.02 Key management					
	12.04 Security of system files	12.04.01 Control of operational software					
		12.04.02 Protection of system test data					
		12.04.03 Access control to program source code					
	12.05 Security in development and support processes	12.05.01 Change control procedures					
		12.05.02 Technical review of applications after operating system changes					
		12.05.03 Restrictions on changes to software packages					
		12.05.04 Information leakage					
		12.05.05 Outsourced software development					
	12.06 Technical Vulnerability Management	12.06.01 Control of technical vulnerabilities					
13.0 Information Security Incident Management	13.01 Reporting information security events and weaknesses	13.01.01 Reporting information security events					
		13.01.02 Reporting security weaknesses					
	13.02 Management of information security incidents and improvements	13.02.01 Responsibilities and procedures					
		13.02.02 Learning from information security incidents					
		13.02.03 Collection of evidence					
14.0 Business Continuity Management	14.01 Information security aspects of business continuity management	14.01.01 Including information security in the business continuity management process					
		14.01.02 Business continuity and risk assessment					
		14.01.03 Developing and implementing continuity plans including information security					
		14.01.04 Business continuity planning framework					
		14.01.05 Testing, maintaining and re-assessing business continuity plans					

ISO 27002 Chapter	Section	Control	Applicable to unit?	Current Condition?	Meets Standard?	Remediation Required?	Risk Level
15.0 Compliance	15.01 Compliance with legal requirements	15.01.01 Identification of applicable legislation					
		15.01.02 Intellectual property rights (IPR)					
		15.01.03 Protection of organizational records					
		15.01.04 Data protection and privacy of personal information					
		15.01.05 Prevention of misuse of information processing facilities					
		15.01.06 Regulation of cryptographic controls					
	15.02 Compliance with security policies and standards, and technical	15.02.01 Compliance with security policies and standards					
		15.02.02 Technical compliance checking					
	15.03 Information systems audit considerations	15.03.01 Information systems audit controls					
		15.03.02 Protection of information systems audit tools					