Process	Sub-Process	What (Objective)	Why (Risk or Exposure)	RETURN TO MENU How (Applicable Controls)	Control Number
K Information Technology	K2 Desktop Computing	Appropriate physical and logical safeguarding techniques are used for portable and desktop information assets.	Laptop and desktop computers containing sensitive data can be lost, stolen, misconfigured, subject to viruses, or otherwise compromised resulting in unauthorized data access, disclosure, damage or destruction.	Laptops are not left unsecured and unattended for extended periods, especially in low traffic areas (or lunch times) where a theft might go unnoticed. Cable Locks are required to physically secure the laptop during the day. When left after normal work hours, laptop is stored in a secure drawer, cabinet, etc.	K2-1.1.1
				PCs connected to the network or that are used to access the County's network have County-approved personal firewall software installed (this includes assets used by non-County employees).	K2-1.1.2
				PCs have a security mechanism that prevents unauthorized access when the PC is left unattended and can automatically activate after a specified period of inactivity. The mechanism is activated anytime the user is away from the PC and is used proactively rather than depending on default time out parameters.	K2-1.1.3
				Encryption is used to store and transmit data based upon the County's policy.	K2-1.1.4
				Logon ID, Passwords and instructions for connections to the network are not carried together in a manner that could be easily used in the event of a theft. Passwords are not written down or displayed in plain site.	K2-1.1.5
				A County approved anti-virus software program is installed and enabled on all personal computers which connect to a County LAN. All personal computers have current versions of anti-virus software and definition files installed and are updated timely.	K2-1.1.6
				PC operating systems are up to date to ensure protection from latest vulnerabilities (version and service pack). PCs are configured to receive automatic updates of security patches, whenever possible.	K2-1.1.7
				Integrity testing of new versions of existing software or additional software is performed prior to implementation on desktop and laptop machines or integration into the County's laptop or desktop image and ensures the software functions as expected, is approved by management and performs without impacting overall computer/network performance.	K2-1.1.8
				Critical data is stored on a regularly backed-up file server, or the data is protected by being part of a timely backup schedule.	K2-1.1.9
				Unapproved removable / portable media (flash drives, DVD/CD, CD burners, etc.) are not used to store, transport, or share sensitive, "confidential" County information assets.	K2-1.1.10
				Removable storage media is protected from unauthorized access, critical data encrypted, and disposed of properly.	K2-1.1.11
				All PCs that have a connection to the network or proprietary information on their local hard drives have a security mechanism installed that prevents unauthorized access when the PC is booted.	K2-1.1.12
				A process is in place for end users to report suspicious activity to a help desk or local IT management. (Suspicious activity may include possible virus infection, security breach, unusual email, unusual system/application behavior, etc.)	K2-1.1.13
				Site security procedures are in place, where appropriate, for laptop / PC removal off premises.	K2-1.1.14