Process	Sub-Process	What (Objective)	Why (Risk or Exposure)	RETURN TO MENU How (Applicable Controls)	Control Number
L General Physical and Logical Security	L1 Physical and Logical Security	County information is retained and disclosed in accordance with County policies and procedures.	County information is used for non-governmental purposes; the County fails to protect personally identifiable information (PII).	Information is safeguarded through physical access restrictions. Restrictions include: badge only access, locked files & locked storage rooms, security cameras and security officers.	L1-1.1.1
				Information is safeguarded through logical (system) access restrictions. Restrictions include password protection, screen saver use, and administrator rights control.	L1-1.1.2
			Confidential information may be inadvertently disclosed.	Document distribution is controlled and all appropriate documents are clearly labeled 'CONFIDENTIAL'.	L1-2.1.1
			Lack of adherence to policies may result in loss of proprietary information / data or confidential information being inadvertently revealed.	The County's policies, such as records retention, are comprehensive and effectively communicated.	L1-3.1.1
				Confidential County information is identified as such, including financial and technical information, County objectives, strategies, forecasts, etc.	L1-3.1.2
				Confidential County Information is shared externally only when an executed Confidentiality Disclosure Agreement (CDA) OR Non-Disclosure Agreement (NDA) is in place.	L1-3.1.3
				When agreements are terminated, a process is in place to retrieve County Confidential information and/or to return Confidential information to the external party.	L1-3.1.4
				County publication and external communication clearance policies and procedures are adhered to.	L1-3.1.5
				Technical information is classified and protected according to County IS Sensitivity Classifications.	L1-3.1.6
				Use of County logos by employees and authorized external parties conforms with recommended practices.	L1-3.1.7
				Communication of any potential loss or misappropriation of proprietary property follows the County's policies.	L1-3.1.8
				Participation in any social networking activities follows County policy.	L1-3.1.9
		Transactions are carried out in accordance with County and Delegation of Authority policies.	Transactions may not have the necessary corporate authorizations; fraud or irregularities could go undetected.	Powers of attorney are reviewed periodically and updated or removed when employees change positions or leave the County.	L1-2.1.1
		Adequate procedures for contingency planning, business continuity and safeguarding of assets exist.	Assets may not be properly safeguarded.	Crisis management plans are documented, communicated, maintained and periodically tested.	L1-3.1.1
				Valuable assets, including intellectual assets and information technology, are protected from unauthorized access or use.	L1-3.1.2
				Packages, briefcases, etc., removed from County facilities are subject to inspection by security personnel according to site security procedures.	L1-3.1.3
		Entrance to County Facilities is restricted as appropriate.	Unauthorized individuals may gain access to County facilities.	Only authorized persons receive badges or other devices that allow access to County facilities.	L1-4.1.1
				Access to facilities is based on job and need.	L1-4.1.2
				Security personnel monitor activity in high risk areas. Monitoring maybe in person or by security device (cameras).	L1-4.1.3