SECURITY PRINCIPLE

Control Objective 1 – Policies

CO1 – DARIC defines and documents its policies for the security of its systems.

	Criteria	Control	Tests Performed	Testing Resu
1.1	DARIC'S security policies are established and periodically reviewed and approved by a designated individual or group.	DARIC'S information security policy addresses both IT and physical security, and it is reviewed and approved annually by the Systems Administrator, Vice President, and President.	Inspected the security policies to ascertain that procedures governing IT and physical security for the in-scope technology and locations were included. Inspected documentation for annual IT and physical security review by the Systems Administrator, Vice President, and President.	No exceptions noted. No exceptions noted.
1.2	DARIC'S security policies include, but may not be limited to, the following matters:	DARIC'S security policies address the following:		
	a. Identifying and documenting the security requirements of authorized users.	Identifying and documenting the security requirements of authorized users.	Inspected the security policies to ascertain they included the matters specified.	No exceptions noted.
	b. Classifying data based on its criticality and sensitivity and that classification is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements.	Classifying data based on its criticality and sensitivity and using the assigned classification to define protection requirements, access rights and access restrictions, and retention and destruction requirements.	Inspected the security policies to ascertain they included the matters specified.	No exceptions noted.

Control Objective 1 – Policies

CO1 – Daric defines and documents its policies for the security of its

	Criteria	Control	Tests Performed	Testing Resu
1.2	c. Assessing risks on a periodic basis.	Assessing risk on a periodic basis	Inspected the security policies to ascertain they included the matters specified.	No exceptions noted.
	d. Preventing unauthorized access.	Preventing unauthorized access.	Inspected the security policies to ascertain they included the matters specified.	No exceptions noted.
	e. Adding new users, modifying the access levels of existing users, and removing users who no longer need access.	Adding new users, modifying the access levels of existing users, and removing users who no longer need access.	Inspected the security policies to ascertain they included the matters specified.	No exceptions noted.
	f. Assigning responsibility and accountability for system security.	Assigning responsibility and accountability for confidentiality and related security.	Inspected the security policies to ascertain they included the matters specified.	No exceptions noted.
	g. Assigning responsibility and accountability for system changes and maintenance.	Assigning responsibility and accountability for system changes and maintenance.	Inspected the security policies to ascertain they included the matters specified.	No exceptions noted.
	h. Testing, evaluating, and authorizing system components before implementation.	Testing, evaluating, and authorizing system components before implementation.	Inspected the security policies to ascertain they included the matters specified.	No exceptions noted.

Control Objective 1 – Policies

CO1 – Daric defines and documents its policies for the security of its

	Criteria	Control	Tests Performed	Testing Resu
1.2	i. Addressing how complaints and requests relating to security issues are resolved.	Addressing how complaints and requests relating to confidentiality and related security issues are resolved.	Inspected the security policies to ascertain they included the matters specified.	No exceptions noted.
	j. Identifying and mitigating security breaches and other incidents.	Handling confidentiality and related security breaches and other incidents.	Inspected the security policies to ascertain they included the matters specified.	No exceptions noted.
	k. Providing for training and other resources to support its system security policies.	Providing for training and other resources to support its system confidentiality and related security policies.	Inspected the security policies to ascertain they included the matters specified.	No exceptions noted.
	l. Providing for the handling of exceptions and situations not specifically addressed in its system security policies.	Providing for the handling of exceptions and situations not specifically addressed in its system security policies.	Inspected the security policies to ascertain they included the matters specified.	No exceptions noted.
	m. Providing for the identification of and consistency with applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements.	Providing for the identification of and consistency with, applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements.	Inspected the security policies to ascertain they included the matters specified.	No exceptions noted.

Control Objective 1 – Policies

CO1 – Daric defines and documents its policies for the security of its

	Criteria	Control	Tests Performed	Testing Resu
1.2	n. Providing for sharing information with third parties.	Providing for sharing information with third parties.	Inspected the security policies to ascertain they included the matters specified.	No exceptions noted.
1.3	Responsibility and accountability for developing and maintaining DARIC'S system security policies, and changes and updates to those policies, are assigned.	DARIC assigns responsibility and accountability for developing and maintaining system security policies to the Security Officer.	Inspected the job descriptions for members of the security administration team to determine whether the description identified the responsibilities of the security administration team for the maintenance and enforcement of the organization's security policy.	No exceptions noted.

Control Objective 2 –

CO2 – Daric communicates its defined system security policies to responsible parties and authorized

	Criteria	Control	Tests Performed	Testing Resu
2.1	DARIC has prepared an objective description of the system and its boundaries and communicated such description to authorized users.	DARIC provides a description of its system, system boundaries, and system processes that includes infrastructure, software, people, and procedures to those people who request it.	Inspected published descriptions of DARIC'S system, system boundaries, and system processes to determine whether the description addressed infrastructure, software, people, procedures, and data for the in-scope technology and locations.	No exceptions noted.
2.2	The security obligations of users and DARIC'S security commitments to users are communicated to authorized users.	DARIC provides ongoing security training to its employees through department meetings and/or emailed instructions. The Company's IT employees are required to annually sign and acknowledge their review of the information security policy. The Company's policies relating to security are reviewed with new employees as part of their orientation, and new employees are required to sign and acknowledge their review of the employee handbook.	Inspected sample of the security meeting minutes to determine whether employees received ongoing security training. For a sample of IT employees, inspected their employee acknowledgements to determine the employees acknowledged their review of the information security policy. For a sample of newly hired employees, inspected the new hire employee acknowledgement forms to determine they signed and acknowledged their review of the employee manual, which included the security policies.	No exceptions noted. No exceptions noted. No exceptions noted.

Control Objective 2 – Communications

CO2 – Daric communicates its defined system security policies to responsible parties and authorized

	Criteri	Contro	Tests Performed	Testing Resu
2.3	Responsibility and accountability for DARIC'S system security policies and changes and updates to those policies are communicated to Company personnel responsible for implementing them.	Written job descriptions have been defined and communicated to the security administration team.	Inspected the job descriptions for the members of the security administration team to determine the description indicated that the security administration team was responsible for the custody and maintenance of the organization's security policy.	No exceptions noted.
2.4	The process for informing DARIC about breaches of the system security and for submitting complaints is communicated to authorized users.	DARIC'S security awareness program trains employees how to identify and report possible security breaches. System alerts, including planned outages and known issues, are communicated via email.	Inspected the security training meeting minutes and determined whether that material described how to identify and report possible security breaches. Inspected a selected system alert email to determine system alerts are communicated to system users.	No exceptions noted. No exceptions noted.
2.5	Changes that may affect system security are communicated to management and users who will be affected.	Planned changes to system components are reviewed, scheduled, and communicated to management as part of the weekly IT maintenance process.	Inspected a sample of weekly IT maintenance schedules and communications to determine planned system changes were included and reviewed and signed off by IT management.	No exceptions noted.

Control Objective 3 –

CO3 – Daric placed in operation procedures to achieve its documented system security objectives in accordance with its defined

	Criteri	Contro	Tests Performed	Testing Resu
3.1	Procedures exist to (1) identify potential threats of disruption to systems operation that would impair system security commitments and (2) assess the risks associated with the identified threats.	A Company-wide risk assessment is performed annually by management includes the following: • Determining business objectives including security commitments • Evaluating the effect of environmental, regulatory, and technological changes on DARIC'S system security • Identifying threats to operations, including security threats, using information technology asset records • Analyzing risks associated with the threats • Determining a risk mitigation strategy • Developing or modifying and	Inspected the annual risk assessment documentation to determine it included the specified procedures.	No exceptions noted.
3.2	Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters:			
	a. Logical access security measures to restrict access to information resources not deemed to be public.	Access to DARIC'S Network is through the use of defined application database user roles.	Inspected user access for a sample users and determined access was authorized and consistent with their role.	No exceptions noted.
		Access granted to users is authorized the department manager, VP of Development or Executive Team.	Inspected Active Directory administrative access granted to authorized individuals.	No exceptions noted.

Control Objective 3 – Procedures

CO3 –Daric placed in operation procedures to achieve its documented system security objectives in accordance with its defined

	Criteri	Contro	Tests Performed	Testing Resul
3.2	a. Logical access security measures to restrict access to information resources not deemed to be public. **(Continued)**	DARIC user role assignments are reviewed by department manager, VP of Product Development or Executive Team monthly.	Inspected a sample of user access reviews noting the review was performed monthly.	No exceptions noted.
	b. Identification and authentication of users.	Unique user identification numbers, names, and passwords are required to authenticate all users to DARIC'S network. Password parameters consist of the following: • Passwords have a minimum of eight characters including one nonalphanumeric character. • Passwords expire every 120 days. • Logon sessions terminate after five failed attempts. • An expired password cannot be recycled for twelve (12) months.	Inspected the password parameters for the system to determine the password parameters were configured with the following specifications: • Passwords have a minimum of eight characters including one nonalphanumeric character. • Passwords expire every 120 days • Logon sessions terminate after five failed attempts. • The passwords cannot be reused for twelve (12) months.	No exceptions noted.
	c. Registration and authorization of new users.	In order for the DARIC'S employees to obtain network access, the department manager must submit a help desk ticket authorizing such access. Proper segregation of duties is considered in granting access privileges based on the user's job role.	Inspected the user access requests for a sample of employees requiring access to the system to determine whether access was authorized and provided for the proper segregation of duties.	No exceptions noted.

Control Objective 3 – Procedures

CO3 –Daric placed in operation procedures to achieve its documented system security objectives in accordance with its defined

	Criteri	Contro	Tests Performed	Testing Resu
3.2	d. The process to make changes and updates to user profiles.	Only authorized Company personnel are able to create or modify user access and user access privileges. The human resources department provides IT personnel with a termination checklist after termination. IT reconciles the report against current system privileges to determine if access has been appropriately removed or disabled.	Inspected a report identifying individuals with access to create or modify user access privileges to determine the access was limited to authorized personnel. Inspected a sample of termination checklists and user accounts to determine user access was appropriately removed or disabled.	No exceptions noted. No exceptions noted.
	e. Distribution of output restricted to authorized users.	Clients accessing the client FTP portal can only view reports for their assigned directory. Administrative access to FTP portal is restricted to authorized personnel.	Inspected FTP system configuration to determine that user access is restricted to assigned directories and administrative access to assign user privileges is restricted to authorized personnel.	No exceptions noted.

Control Objective 3 – Procedures

CO3 –Daric placed in operation procedures to achieve its documented system security objectives in accordance with its defined

	Criteri	Contro	Tests Performed	Testing Resu
3.2	f. Restriction of access to offline storage, backup data, systems, and media.	The Company restricts access to offline storage, backup data, systems, and media to authorized individuals. Data and media are backed up to an encrypted hard drive that is password protected and secured in a locked case offsite.	Inspected the backup encryption configuration to determine access to data is restricted to authorized individuals.	No exceptions noted.
	g. Restriction of access to system configurations, super user functionality, master passwords, powerful utilities, and security devices (e.g., firewalls).	Administrative access to the DARIC' firewall is restricted to the System Administrator. All firewall changes are logged by the security incident and event (SIEM) utility and are reviewed by the security administration team. Administrative access to Active servers and databases is restricted to authorized personnel. A list of all master passwords is in a password-encrypted database.	Inspected the firewall system configuration and access listing to determine access was restricted to authorized personnel and changes logged. Inspected the Active Directory and servers' access listings to access was restricted to authorized personnel. Inspected the database to determine master passwords maintained in an encrypted database.	No exceptions noted. No exceptions noted. No exceptions noted.

Control Objective 3 – Procedures

CO3 –Daric placed in operation procedures to achieve its documented system security objectives in accordance with its defined

	Criteri	Contro	Tests Performed	Testing Resu
3.3	Procedures exist to restrict physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers.	Physical access to the data centers that house the DARIC'S IT resources, servers, backup media, and related hardware, such as firewalls and routers, is restricted to authorized individuals by card key systems.	Inspected key card system user listing to the data center to determine key card systems restricted access to authorized individuals.	No exceptions noted.
		Requests for physical access privileges to the Company's computer facilities require approval from authorized IT management personnel.	There were no new users granted access during the audit period.	No testing performed.
		Documented procedures exist for the identification and escalation of potential physical security breaches.	Inspected written security policies and ascertained the policies addressed the identification and escalation of potential physical	No exceptions noted.

Control Objective 3 – Procedures

CO3 –Daric placed in operation procedures to achieve its documented system security objectives in accordance with its defined

	Criteri	Contro	Tests Performed	Testing Resu
3.4	Procedures exist to protect against unauthorized access to system resources.	Virtual private networking (VPN) software is used to restrict remote access. Users are authenticated by the VPN server through user identification names, and passwords, and a preshared key.	Inspected the VPN configurations to determine user identification numbers, names, and passwords were required.	No exceptions noted.
		DARIC uses firewalls to prevent unauthorized network access.	Inspected the network diagram to determine the design of the system included firewalls to prevent unauthorized network access.	No exceptions noted.
		The Company contracts with third-party security providers to conduct quarterly security reviews and vulnerability assessments. Results and recommendations are communicated to and addressed by management.	For a sample of months, inspected the security review and vulnerability assessment reports to determine the assessments were performed and communicated.	No exceptions noted.
3.5	Procedures exist to protect against infection by computer viruses, malicious code, and unauthorized software.	DARIC uses anti-virus software on all Windows-based desktops, laptops, and servers. These systems are configured to query the anti-virus repository daily to retrieve the latest antivirus definitions.	Inspected the anti-virus software configurations to determine the software was configured to retrieve the latest anti-virus definitions on a daily basis.	No exceptions noted.
		The Company uses a SIEM utility to identify and record any computer viruses identified on the Company's network	Observed the SIEM utility to determine management had recorded any identified computer viruses.	No exceptions noted.

Control Objective 3 – Procedures

CO3 –Daric placed in operation procedures to achieve its documented system security objectives in accordance with its defined

	Criteri	Contro	Tests Performed	Testing Resu
3.6	Encryption or other equivalent security techniques are used to protect user authentication information and the corresponding session transmitted over the Internet or other public networks.	DARIC'S employees have the ability to encrypt email attachments using a secure WinZip or PGP encryption. The DARIC'S remote access VPN uses Layer 2 Tunneling Protocol and Internet Protocol Security (L2TP IPSec) to encrypt all remote sessions.	Inspected system setting on the email server to determine emails could be encrypted when required. Inspected the VPN configurations to determine Layer 2 Tunneling Protocol and Internet Protocol Security (L2TP IPSec) encryption was used.	No exceptions noted. No exceptions noted.
Criteria related to execution and incident management used to achieve objectives				
3.7	Procedures exist to identify, report, and act upon system security breaches and other incidents.	User entities are provided with instructions for communicating potential security breaches to the information security team. When a potential security incident is detected, a defined incident management process is initiated by authorized personnel. Corrective actions are implemented in accordance with defined policies and procedures	Inspected the instructions provided to user entities to determine they included protocols for communicating potential security breaches. Inspected the written incident management procedures to determine whether the procedures included a process for handling the security incident.	No exceptions noted. No exceptions noted.

Control Objective 3 – Procedures

CO3 –Daric placed in operation procedures to achieve its documented system security objectives in accordance with its defined

	Criteri	Contro	Tests Performed	Testing Resu
Criteria related to the system components used to achieve the objectives				
3.8	Procedures exist to classify data in accordance with classification policies and periodically monitor and update such classifications as necessary.	DARIC has a defined information classification scheme for the labeling and handling of data. The Company classifies data into two levels: Public and Sensitive Data.	Inspected the data classification policy to determine there was a documented classification scheme for labeling and handling data.	No exceptions noted.
3.9	Procedures exist to provide that issues of noncompliance with security policies are promptly addressed and that corrective measures are taken on a timely basis.	Security incidents are reported to Executive Team and follow the Incident Response Policy. Employees found to be in violation of DARIC'S information security policy are subject to disciplinary action up to and including termination of employment.	There were no security incidents during the audit period. Inspected the security policy to determine the policy included procedures for employees in violation of the policy.	No testing performed. No exceptions noted.
3.10	Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system security policies to enable authorized access and to prevent unauthorized access.	DARIC has a formalized security and systems development methodology that includes project planning, design, testing, implementation, maintenance, and disposal or decommissioning.	Inspected the security and systems development methodology policy to determine it included project planning, design, testing, implementation, maintenance, and disposal or decommissioning.	No exceptions noted.

Control Objective 3 – Procedures

CO3 –Daric placed in operation procedures to achieve its documented system security objectives in accordance with its defined

	Criteri	Contro	Tests Performed	Testing Resu
3.11	Procedures exist to provide that personnel responsible for the design, development, implementation, and operation of systems affecting security have the qualifications and resources to fulfill their responsibilities.	DARIC has written job descriptions specifying the responsibilities and academic and professional requirements for key job positions. Hiring procedures include a comprehensive screening of candidates for key positions and consideration of whether the candidate's credentials are commensurate with the position. New personnel are offered employment subject to background checks.	For a sample of positions, inspected written job descriptions to determine the job descriptions included responsibilities and academic and professional requirements. For a sample of new employees, inspected the results of background checks to determine a background check was performed.	No exceptions noted. No exceptions noted.

Control Objective 3 – Procedures

CO3 –Daric placed in operation procedures to achieve its documented system security objectives in accordance with its defined

	Criteria	Control	Tests Performed	Testing Resu
Change management-related criteria applicable to the system's security				
3.12	Procedures exist to maintain system components, including configurations consistent with the defined system security policies.	DARIC maintains a documented change management and patch management process.	Inspected the change and patch management policies to determine there were documented procedures.	No exceptions noted.
		Servers are reviewed monthly by the security administration team to determine if required vendor security patches have been applied.	For a sample of months, inspected management's server review documentation to determine the security patches were applied.	No exceptions noted.
		The Company contracts with third parties to conduct quarterly security reviews and vulnerability assessments. Results and recommendations for improvement are reported to management. Management develops a plan for action for each recommendation and follows up on open recommendations on a regular basis.	For a sample of months, inspected the security review and vulnerability assessment reports to determine the assessments were performed, communicated, and addressed by management.	No exceptions noted.

Control Objective 3 – Procedures

CO3 –Daric placed in operation procedures to achieve its documented system security objectives in accordance with its defined

	Criteri	Contro	Tests Performed	Testing Resu
3.13	Procedures exist to provide that only authorized, tested, and documented changes are made to the system.	DARIC maintains a formally documented change management process. Changes to hardware, operating system, and system software are authorized, tested (when applicable), and approved by appropriate personnel prior to implementation. Changes in system infrastructure and software are developed and tested in a separate development or test environment before implementation. Additionally, developers do not have the ability to migrate changes into production environments.	Inspected the change management policy for hardware, operating system, and system software to determine procedures were documented to include authorization, tested (when applicable), and approved prior to implementation. Inspected documentation of the system infrastructure architecture to determine a separate development or test environment existed from the production environment. Inspected the access list to the change management tools to determine access to migrate changes to production was appropriate based on job responsibilities and that developers did not have the ability to migrate changes into production.	No exceptions noted. No exceptions noted. No exceptions noted.
3.14	Procedures exist to provide that emergency changes are documented and authorized timely.	Emergency changes follow the standard change management process, but at an accelerated timeline. Prior to initiating an emergency change, all necessary approvals are obtained and documented.	There were no emergency changes during the audit period.	No testing performed.

Control Objective 4 –

CO4 – Daric monitors the system and takes action to maintain compliance with its defined system security

	Criteri	Contro	Tests Performed	Testing Resu
4.1	DARIC'S system security is periodically reviewed and compared with the defined system security policies.	External vulnerability assessments are performed on a monthly basis, and management initiates corrective actions for identified vulnerabilities. DARIC performs monthly user access reviews.	Inspected a sample of vulnerability assessments noting monthly performance. Obtained a sample of monthly user access reviews, noting review by management.	No exceptions noted. No exceptions noted.
4.2	There is a process to identify and address potential impairments to DARIC'S ongoing ability to achieve its objectives in accordance with its defined system security policies.	DARIC uses a SIEM utility to capture the following critical security events: • Daily intrusion detection system (IDS) or intrusion prevention system (IPS) attacks • Critical IDS or IPS alerts • Servers not reporting in the past 15 minutes • Firewall configuration changes Reports are logged and reviewed by the systems administrator.	Selected a sample of SIEM logs, noting capture of critical security events and monitoring reports are available to systems administrator.	No exceptions noted.