INFORMATION SECURITY PLAN

November 23, 2020

TOOELE COUNTY

Table of Contents

IS-01 - Information Security Policy 6
1.1 Policy Source 6
1.2 Purpose 6
1.3 Scope 6
1.4 Information Security Roles and Responsibilities 6
1.4.1 Leadership Roles and Responsibilities 6
1.4.2 Worker Roles and Responsibilities 6
1.5 Policy 7
1.5.1 Policy Management 7
1.5.2 Exceptions 7
1.5.3 Programs 7
1.5.4 Program Maintenance 8
1.5.5 Program Compliance 8
1.6 Violations 8
1.7 Related Documents 9

IS-02 – Acceptable Use Policy 10
2.1 Purpose 10
2.2 Scope 10
2.3 Policy 10
2.3.1 Acceptance of Shared Responsibility 10
2.3.2 Minimum Acceptable Employee Practices 10
2.3.3 Communications Systems 11
2.3.4 Internet and Intranet 11
2.3.5 Protecting Internal Systems and Equipment 12
2.3.6 Telecommuting 12
2.4 Related Documents 12

IS-03 – Identity Management Policy 13
3.1 Purpose 13
3.2 Scope 13
3.3 Policy 13
3.3.1 User IDs and Accounts 13
3.3.2 Access Credentials 14
3.3.3 Password Requirements 14
3.4 Related Documents 15

IS-04 – Access Management Policy 16
4.1 Purpose 16
4.2 Scope 16
4.3 Policy 16
4.3.1 Access Control Requirements 16
4.3.2 Access Approval 16
4.3.3 Access Privileges 16
4.3.4 Special System Privileges 17
4.3.5 Access Records 17
4.4 Related Documents 17

IS-05 – Asset Management Policy 18
5.1 Purpose 18
5.2 Scope 18
5.3 Policy 18

5.3.1 Asset Procurement 18
5.3.2 Asset Inventory 19
5.3.3 Security Requirements 20
5.3.4 Equipment Decommissioning and Disposal 20
5.4 Related Documents 20

IS-06 – Information Technology Asset Disposal Policy 21
6.1 Purpose 21
6.2 Scope 21
6.3 Policy 21
6.3.1 Asset Disposal 21
6.4 Related Documents: 22

IS-07 – Hardware Sanitization Policy 23
7.1 Purpose 23
7.2 Scope 23
7.3 Policy 23
7.3.1 Requirements 23
7.3.2 Scenarios for Disposal 23
7.3.3 Technical Guidance on Sanitization 24
7.4 Related Documents 24

IS-08 – Mobile Computing Security Policy 25
8.1 Purpose 25
8.2 Scope 25
8.3 Policy 25
8.3.1 Mobile Device Configuration 25
8.3.2 Enterprise Device Management (EDM) 25
8.3.3 Physical Protection 26
8.4 Related Documents 26

IS-09 – Physical Security Policy 27
9.1 Purpose 27
9.2 Scope 27
9.3 Policy 27
9.3.1 Security of Buildings and Facilities 27
9.3.2 Access Badges 27
9.3.3 Visitors 28
9.3.4 Data Centers 28

IS-10 – Firewall Management Policy 30
10.1 Purpose 30
10.2 Scope 30
10.3 Policy 30
10.3.1 Requirements 30
10.3.2 Implementation and Operation 30
10.3.3 Change Management 31

IS-11 – Information Classification and Handling Policy 32
11.1 Purpose 32
11.2 Scope 32
11.3 Policy 32
11.3.1 Roles and Responsibilities 32
11.3.2 Information Classification 32
11.3.3 Electronic Data Destruction 34

11.3.4 Disposal of Hardcopy Documents 34
IS-12 – Backup and Recovery Policy 35
12.1 Purpose 35
12.2 Scope 35
12.3 Policy 35
12.3.1 Backup Types and Schedules 35
12.3.2 Retention and Storage 35
12.3.3 Testing and Review 36
12.4 Related Documents 36
IS-13 – Third-Party Risk Management Policy 37
13.1 Purpose 37
13.2 Scope 37
13.3 Policy 37
13.3.1 Vendor Selection 37
13.3.2 Vendor Contracts 38
IS-14 – Vulnerability and Patch Management Policy 39
14.1 Purpose 39
14.2 Scope 39
14.3 Policy 39
14.3.1 Network Inventory 39
14.3.2 Internal Vulnerability Scans 39
14.3.3 External Vulnerability Scans 40
14.3.4 Vulnerability Remediation 40
IS-15 – Information Security Awareness Policy 41
15.1 Purpose 41
15.2 Scope 41
15.3 Policy 41
15.3.1 Roles and Responsibilities 41
15.3.2 Requirements 41
IS-16 – Secure Application Development Policy 43
16.1 Purpose 43
16.2 Scope 43
16.3 Policy 43
16.3.1 Secure Application Development 43
16.3.2 Code Management 43
16.3.3 Production Data in Test Environments 44
16.3.4 Code Changes 44
16.3.5 Default Settings 44
IS-17 – Charter: Information Security Committee 45
17.1 Purpose 45
17.2 Authority 45
17.3 Scope 45
17.4 Composition 45
17.5 Committee Responsibilities 45
17.6 Meeting Schedule 46
17.7 Decision Model 46
17.8 Meeting Agenda 46
17.9 Attendance 47
17.10 Communication 47

Appendix A- Information Handling Requirements 48
Appendix B – Glossary of Terms 49
Appendix C – Revision History 56

IS-01 - Information Security Policy

1.1 Policy Source

This policy and all other information security policies are issued under the authority of the Tooele County Information Security Committee. Inquiries concerning this policy should be directed to the Information Technology Director.

1.2 Purpose

This policy establishes the minimum requirements and responsibilities for protecting Tooele County information systems and data from potential threats. It defines the components of the Tooele County Information Security Program, establishes roles and responsibilities, and specifies the processes for making changes and dealing with violations.

1.3 Scope

This policy applies to all Tooele County computer systems and facilities, and to all users with access to Tooele County information assets.

1.4 Information Security Roles and Responsibilities

1.4.1 Leadership Roles and Responsibilities

Information Technology Department - The Information Technology Director is responsible for establishing and maintaining county-wide information security policies, standards, guidelines, and procedures, in conjunction with the Tooele County manager and the Tooele County Attorney.

Information Security Committee (ISC) - The ISC will meet monthly to review information security for Tooele County. The ISC will approve and review information security projects, approve new or modified information security policies, and perform other necessary high-level information security management activities.

Information Security Resources – Tooele County management must allocate sufficient resources and staff to adequately address information security.

Clear Assignment of Control Accountability – Tooele County management must clearly assign and document accountability for establishing and maintaining information security controls. The personnel responsible for security controls must keep management informed of the effectiveness of those controls.

1.4.2 Worker Roles and Responsibilities

Information Owners - Individuals assigned as Owners are responsible for making sure information is stored securely in the correct location with appropriate access controls. Owners approve data sharing agreements. Each information system and its data must have a designated Owner.

Information Custodians - Custodians have physical or logical possession of information systems. They manage system operations and maintain the security measures defined by information Owners. Each information system and its data must have one or more designated Custodians.

Information Users - Users will access and manage information appropriately. They must understand and comply with all Tooele County Information Security policies, procedures, and standards. They should direct questions about the handling of specific types of information to the Custodian or Owner. All users will receive basic cybersecurity awareness training within two weeks of their hire date. Failure to complete cybersecurity training within the two-week period will result in the user's access being disabled until such time as the training has been completed. Additional cybersecurity training may be administered periodically.

1.5 Policy

1.5.1 Policy Management

Policy Distribution - Tooele County must make its information security policies available to the appropriate users and relevant external parties (such as auditors) who have a legitimate business need.

Worker Acceptance of Security Policies - All Tooele County users must review and certify acceptance of the information security policies upon their hire date and annually thereafter.

Policy Annual Review - Tooele County Information Security Policies must be reviewed annually by the Information Technology Director and approved by the Information Security Committee. The review should include any decisions to revise policy, improve security management, improve security controls and objectives, and adjust allocation of security resources or responsibilities.

1.5.2 Exceptions

Policy Exceptions - Exceptions to information security policies are rare and will be granted only after assessing the risks of being out of compliance. Exceptions are granted only in the short term unless and until approved by the Information Security Committee.

Periodic Exceptions Review - All documented and approved security policy exceptions must be reviewed by the Information Security Committee at least annually.

1.5.3 Programs

Information Security Program - Tooele County will establish a comprehensive Information Security Program to secure its information assets.

Information Privacy Program - Tooele County Information Technology Department will establish an Information Privacy Program to secure user personal information against unauthorized use or disclosure, including PII, PHI, and any other type of personally identifiable information.

Cybersecurity Risk Management Program - Tooele County Information Technology Department must establish a regular program for determining compliance with security policies and identifying areas of risk. The program will also include an insurance policy, to be reviewed annually by the Tooele County Information Security Committee.

Information Security Awareness Program - Tooele County Information Technology Department must establish an Information Security Awareness training program for all users with access to Tooele County information assets.

1.5.4 Program Maintenance

Annual Program Review - The various information security programs must be reviewed by Tooele County management annually, or whenever there is a material change to the organization or infrastructure.

Change Considerations - Changes that may trigger updates to the information security programs and policies may include changes to technologies, information classifications, the nature and extent of the threat environment, business arrangements (for example, mergers, alliances, or joint ventures), or information systems (such as new configurations, connectivity, or software).

Annual Report - Each year the Information Technology Director must submit to Tooele County Management an information security report that includes:

a. the status of programs.
b. an updated risk assessment and analysis.
c. management decisions about the level of risk mitigation and residual risk accepted.
d. results of testing of key controls.
e. management response to any identified deficiencies.
f. recommendations for program changes.
g. report on significant incidents, breaches, etc. that have happened during the reportable year.

1.5.5 Program Compliance

Laws, Regulations, and Contractual Requirements - Tooele County must identify and comply with all relevant statutory, regulatory, and contractual requirements related to securing information stored, processed, or transmitted by Tooele County.

Compliance Audits - An independent review of information systems security must be conducted annually to determine the adequacy of security controls and the level of compliance with those controls.

1.6 Violations

Reporting Violations - A user who becomes aware of an information security policy violation should report it to his or her manager. Managers should verify the violation and then take appropriate action. Serious violations should be reported to the Human Resources

Department as soon as possible. Any user who is requested to undertake an activity which he or she believes is in violation of this policy, must provide a written complaint to his or her manager, any other manager, or the Human Resources Director as soon as possible.

Liability Limitations - Any violation of this or any other information security policy may result in disciplinary action, up to and including termination of employment, see Personnel Policies and Procedures section 24. Tooele County reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. To the extent permitted by law, Tooele County reserves the right not to defend or pay any damages awarded against users that result from violation of this policy.

1.7 Related Documents

Acceptable Use Policy

IS-02 – Acceptable Use Policy

2.1 Purpose

This policy establishes the minimum acceptable practices, requirements, and responsibilities for the use and protection of Tooele County information assets.

2.2 Scope

This policy applies to all computer systems and facilities owned or leased by Tooele County
This policy applies to all users with access to Tooele County information assets.

2.3 Policy

2.3.1 Acceptance of Shared Responsibility

Protecting Information - Protecting Tooele County information systems and data requires active participation from everyone with access privileges.

Required Participation - All users must follow the requirements of this and all other applicable information security policies, standards and procedures when performing duties on behalf of Tooele County and its customers.

Cybersecurity Training - All users must take the Tooele County Information Technology Department cybersecurity training course before receiving access to Tooele County information systems. All cybersecurity training must be reviewed Semi-Annually.

2.3.2 Minimum Acceptable Employee Practices

Personal Use of Information Systems - Tooele County information systems are intended to be used for business purposes.

User IDs and Passwords - Users must manage and protect user accounts and IDs as explained in the Identity Management Policy. When creating and using passwords, users must comply with the requirements in the Identity Management Policy.

Workstation Configuration - Users must not make changes to the basic workstation configuration or security tools. Only authorized software should be installed. Refer to the Asset Management Policy for additional guidance.

Physical Security - To ensure the safety and security of Tooele County equipment and facilities, users must follow the requirements in the Physical Security Policy.

Sensitive Information - Users having custody of Tooele County sensitive information must protect it from unauthorized disclosure and must handle it in accordance with the Information Classification and Handling Policy.

Duty to Report Concerns - All users have a duty to promptly report concerns about information security to the Information Technology Department as outlined in the Incident

Management and Reporting Policy. Examples of reportable matters include lost or stolen equipment, suspicious email or phone calls, or unusual computer behavior or activity.

User Installation of Software - Users must not install software on computers, network servers, or other machines without authorization from the Information Technology Department.

Software Copying - Users must not share or make unauthorized copies of software provided by Tooele County.

System Resource Consumption - Users must not run any program or process that is likely to consume significant system resources or otherwise interfere with business activities.

2.3.3 Communications Systems

Use of Email and IM - Tooele County email and instant messaging systems are intended primarily for business purposes. Users must not use official email or IM applications in ways that could cause embarrassment or liability to Tooele County. Users must use the approved County email system and their official accounts for sending and receiving emails related to County business.

Spam - Users must not send unsolicited bulk email (spam) unless as part of authorized work activity. Unauthorized senders will be subject to disciplinary action, up to and including termination.

Suspicious Email - Users that receive suspicious email (phishing) should report it to the Information Technology Department.

Non-business Use of County Email Addresses - Tooele County email addresses must not be used in conjunction with any non-Tooele County account, for example, as a login ID for a personal online account.

Offensive Messages - Offensive communications received by a user must be reported to their manager and the Human Resources Department.

Identity Misrepresentation - Users must not misrepresent their own or another person's identity on any Tooele County electronic communications.

2.3.4 Internet and Intranet

Personal Use of Internet - Internet access is provided primarily as a tool to accomplish work. Personal use is allowed as defined in Tooele County Personnel Policies & Procedures Section 21. **Internet use must not degrade the operation of** Tooele County information systems.

No Expectation of Privacy - Users must avoid inappropriate use of County provided Internet access. Internet browsing through Tooele County systems is filtered, monitored, logged, and reported on a regular basis. End-users should have no expectation of privacy when accessing the Internet through any application.

Public Computers - Users must not connect to Tooele County systems from a shared public computer or terminal.

Large Internet Downloads - Internet users must not use video streaming facilities or download large files that may degrade the operation of Tooele County information systems without advance approval by the Information Technology Department.

Social Networking Sites - Users must not use Tooele County systems to access social networking sites or post county information there unless required as part of official duties.

2.3.5 Protecting Internal Systems and Equipment

Objectionable Content - All forms of offensive, defamatory, obscene, pornographic, or harassing content are strictly prohibited on Tooele County computers and networks.

Malicious Software - Users must not intentionally introduce malicious software onto Tooele County computers or networks. Users who suspect a device has been infected by a virus must immediately contact the Information Technology Department.

Hacking - Unless specifically approved in advance and in writing by the ISC, users must not engage in hacking or penetration testing activities.

Safeguarding Computers - Users must not leave laptops, notebooks, handhelds, or other portable devices unattended at any time in non-secure areas. In secure areas, computers or devices must always be logged out or locked when left unattended. When traveling by air, users must not leave computers or devices in checked airline luggage.

Encryption - Users must not set up, remove, or disable encryption protection on computers without authorization from the Information Technology Department.

Personally Owned Computer Systems - Users must not bring personally owned computers, peripherals, or software into Tooele County facilities without prior authorization from the Information Technology Director.

2.3.6 Telecommuting

Telecommuting Equipment - Telecommuting users must use computer equipment provided by Tooele County unless other equipment has been approved and is compatible with Tooele County information systems and controls. Tooele County owned computer equipment is mandatory when accessing Tooele County systems and controls through Palo Alto VPN. Personal devices are allowed when accessing Tooele County systems and controls through VMWare Horizon environment.

Protection of County Equipment - Precautions must be taken to protect Tooele County hardware, software, and information from theft, damage, or misuse at remote work sites.

2.4 Related Documents

Information Security Policy

IS-03 – Identity Management Policy

3.1 Purpose

This policy defines the control requirements for the secure management of user identities and accounts on Tooele County computer and communications systems.

3.2 Scope

This policy applies to all users of Tooele County computer systems and assets.

3.3 Policy

3.3.1 User IDs and Accounts

ID and Account Provisioning - All user accounts will be provisioned and managed by the Information Technology Department. All user Accounts must be audited at least once a year.

User Account Agreements - Before being given a Tooele County information systems account, all users must complete an agreement to comply with applicable information security and privacy requirements.

Unique User IDs and Passwords - Each user must have a unique user ID and personal password. Each ID must identify only one user and be connected solely with the user it was assigned to.

Shared User IDs - Shared or group user IDs are prohibited.

Systems Administrator User IDs - Systems administrators must have at least two user IDs, one that provides normal user privileges for day-to-day work, and one that provides privileged access. All privileged administrator accounts must use multi-factor authentication.

Local Administrator Accounts – Local Administrator Accounts are not allowed on Tooele County assigned equipment, unless otherwise approved by the Information Technology Department. Normal user accounts must not include any local administrative functions.

Vendor, Contractor and Seasonal/Temp Accounts - All vendor, contractor, and Seasonal/Temp accounts must be approved by the Information Technology Department and must include an expiration date.

Changes to Accounts - Changes to user account names, IDs, or other identifier objects must be authorized by the user's manager.

User Status Changes - User accounts should be reviewed at least annually to check for changes to user status or inactive or expired accounts. Access for terminated users must be revoked immediately.

3.3.2 Access Credentials

User Responsibilities - Users are responsible for all activity performed with their personal accounts, user IDs, passwords, or other access credentials. No one is permitted to share or perform any activity with another user's accounts, IDs, or credentials.

Storing Access Credentials - Authentication credentials must not be stored on computers, smart phones, or other portable devices unless encrypted and protected by some form of access control. Never write down a password and store it near a computer or other access device. Never store passwords in communications programs, Internet browsers, or other software. Never store PINs, passwords, user IDs, or other types of access information in script files.

Multi-factor Authentication - Multi-factor authentication is required for accounts with elevated privileges and is strongly recommended for all accounts.

Encryption - All passwords must be encrypted and communicated using a secure connection.

Suspected Password Disclosure - Passwords that are known or suspected of being compromised must be changed immediately and the disclosure promptly reported to the Information Technology Department.

Password Obfuscation - When entering credentials, the password field must not completely display the password.

Temporary Passwords - Temporary passwords must be set to force a password change before completing the first login process.

Password Entry Errors - When one of the login credentials is incorrect, error messages must not indicate which of the pair is wrong.

Access Lockout - Authentication systems must implement some form of intruder lockout to inhibit password guessing attacks, such as a minimum number of failed authentication attempts.

Generic or Default Accounts/Passwords - All vendor-supplied default accounts or passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems must be changed before a resource is used in production. Default usernames should also be changed where possible.

Dynamic Password Tokens and Smartcards - Dynamic password tokens such as security key fobs and smartcards must not be stored in the same case as portable computers.

3.3.3 Password Requirements

Password Creation - Users must not use predictable or easily guessed passwords such as words in a dictionary, forms of user IDs, common character sequences, words commonly associated with Tooele County terminology, or personal details.

Password Length - Passwords must be at least 12 characters long.

Special Characters - Passwords must contain at least one number and one upper case character.

Password Expiration - Passwords will expire every 90 days and must be changed. The passwords of privileged accounts will expire every 90 days. During changes, the previous 5 passwords will be disallowed.

No Reuse - Tooele County user account passwords must not be used with any other account.

3.4 Related Documents

Access Management Policy

IS-04 – Access Management Policy

4.1 Purpose

This policy defines the requirements for managing authorization to access to Tooele County information assets, including but not limited to networks, applications, data, computers, or other devices or services.

4.2 Scope

This policy applies to all Tooele County computer systems and facilities and all users of Tooele County information assets.

4.3 Policy

4.3.1 Access Control Requirements

Access Capabilities and Commands - Tooele County access control systems must grant end users only the system capabilities and commands they have been authorized to have.

Production Restrictions - Access controls must restrict general users from being able to modify networking, server, or workstation systems in production environments.

Access Control Malfunction - If an access control system malfunctions, it must automatically default to denial of privileges to end users.

4.3.2 Access Approval

Security Requirements Agreement - All users must agree to comply with Tooele County information security and privacy requirements.

Access Request - An access request must be completed for each user before access privileges are granted. Requests must be approved by the user's manager and Information Technology Department. Requests for changes to privileges must go through the same process.

Access to Sensitive Information - Requests for access to sensitive information must be approved by the Information Owner.

4.3.3 Access Privileges

Privilege Limitations - Access privileges must be limited based on the principles of need-to-know and least privilege. Users will be given access only to the resources and capabilities required for their work.

Information Security Training - In order to maintain access privileges, all users must complete the appropriate information security training module(s) on a semi-annual basis.

Access Review - The system privileges of each user must be reviewed annually by the user's immediate manager to determine if they are still appropriate for current duties.

Revocation of Access Privileges - Access privileges may be removed where no longer needed or where it is determined that certain policy violations have occurred.

4.3.4 Special System Privileges

Special Privileges - Elevated system privileges must be approved in advance by a user's manager, the Information Owner, and the Information Custodian. Special privileges will be given only as required for legitimate business purposes and only at the minimum level required to accomplish the assigned work.

Access to Personally Identifiable Information (PII) - Users are not allowed to access personally identifiable information (PII) or sensitive personal information (SPI) – such as credit card numbers, credit references, and social security numbers – except as needed to perform their jobs.

Operating System Command Access - End users must not be given privileges to invoke elevated operating system-level commands.

4.3.5 Access Records

Access Records - Current records must be kept of all systems where users have access, and of the privileges granted to each user. These records must be securely maintained for a minimum of 5 years with the exception of Elected Officials and Appointed positions that have no expiration date.

Access Change Logs - All Tooele County production systems must log any changes to user access privileges.

4.4 Related Documents

Identity Management Policy

IS-05 – Asset Management Policy

5.1 Purpose

This policy establishes the minimum requirements and responsibilities to protect Tooele County information assets, prevent misuse and loss, establish the basis for audits and self-assessments, and preserve Tooele County Management options and legal remedies in the event of loss or misuse.

5.2 Scope

This policy applies to all Tooele County information assets, and to all individuals who have been given access to those resources.

5.3 Policy

5.3.1 Asset Procurement

Hardware and Software Procurement - All IT hardware and software must be approved by and procured through the Tooele County Information Technology Department from approved vendors. These approved vendors should provide both maintenance services and warranties.

Hardware Purchases. Hardware Purchase Requests are made through the Information Technology Help Desk. Hardware may only be purchased for one of the following events:

a. **New Hires** - The Information Technology Department will procure new equipment or supply from available inventory. Vendors and Contractors "User Access Requests" must be submitted and reviewed by the Information Technology Department at least 10 days prior to the start of work and they must provide their own hardware. The hardware must be approved by the Information Technology Department prior to the start of work.

b. **Equipment End of life or Failures** - Hardware refresh budgets are the responsibility of the County Auditor and the Department Head and are allocated annually for estimated replacement of equipment expiring during the coming budget year.

c. **Lost or Stolen Equipment** - The Information Technology Department will procure new equipment or supply from available inventory.

d. **Approved Projects** - Requests are submitted through the Information Technology Department and are managed as part of project budget allocations.

Software Purchases - Software includes all applications, utilities, operating systems, databases, cloud services (SAAS, IAAS, and PAAS), and products consumed by Tooele County.

a. **New Hires -** New or reassigned licenses are procured and paid for under existing licensing agreements.

b. **New or Upgraded Software -** New software purchases and upgrades to existing applications are requested through the Information Technology Department. Cloud services subscriptions are budgeted for annually based on headcount estimates.

Overages due to increased licenses should be paid for by the requesting Department.

5.3.2 Asset Inventory

Inventory Requirements - The Information Technology Department must maintain the enterprise IT Asset Inventory with all discoverable hardware and software assets. This inventory shall include all assets, whether connected to the organization's network or not.

Maintain Secure Images - Maintain secure images or templates for all systems based on approved configuration standards. Store the master images and templates on securely configured servers to ensure that only authorized changes to the images are possible.

Encryption - All laptops and other portable computing devices must be configured with full disk encryption. All PCs or other equipment used offsite must also be encrypted.

Deploy System Configuration Management Tools - Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.

Active Discovery - The Information Technology Department will use an active discovery tool to identify devices connected to the Tooele County network and update the hardware asset inventory with newly discovered assets.

Inventory Data and Access Control - The Information Technology Department shall use port-level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.

Unauthorized Assets - Unauthorized assets must either be removed from the network, quarantined, or approved and added to the inventory in a timely manner.

Asset Attributes - Where possible, the Tooele County asset inventory should include the following attributes for each asset:

- **a.** network address
- **b.** hardware address
- **c.** machine name
- **d.** location
- **e.** data asset owner
- **f.** department

Reporting Lost or Stolen Equipment - Tooele County users must report lost or stolen equipment to the Information Technology Department within 24 hours. All lost or stolen equipment may be investigated internally through the Tooele County Sheriff's Office or other outside Public Safety Agency in the event of a conflict.

5.3.3 Security Requirements

Security Configuration - Tooele County will maintain documented security configuration standards for all authorized operating systems and software. All computer and communication equipment must be provisioned with an approved security configuration.

Security Classification - All infrastructure assets will be assigned one of the security classifications described in the Information Classification and Handling Policy.

Updates and Patches - The most recent security updates and patches must be installed as soon as practical without interfering with business operations.

Logging and Monitoring - Appropriate logging and monitoring must be enabled to detect possible unauthorized activity. Security-related events must be logged, and audit trails saved.

VPN - An approved VPN or other remote access application must be used to access to internal networks from an outside location.

Unused Services - Services and applications that will not be used must be disabled.

5.3.4 Equipment Decommissioning and Disposal

Decommissioned Equipment - The Information Technology Department is responsible for the disposal of property no longer needed for business activities. An inventory of all decommissioned equipment must be maintained that includes a record of all actions taken to clear information from memory, hard drives, and all other forms of storage.

Equipment Recycling or Reassignment - Equipment designated as surplus must be restored to its original configuration and recycled or sold. Equipment recycled or sold must have hard drives removed. Disk drives in reassigned equipment must be securely reimaged. Mobile phones should be reset to default settings. Removable memory should be disposed of separately.

Used Equipment Release - Before disposal or recycling, the Information Technology Department must validate that sensitive information has been removed. Equipment must have a label attached stating that the hard drive has been properly sanitized.

Employee Restriction - Tooele County employees shall not profit from the disposal of IT assets.

5.4 Related Documents

Information Technology Asset Disposal Policy

IS-06 – Information Technology Asset Disposal Policy

6.1 Purpose

This policy establishes and defines the standards, procedures, and restrictions for the disposal of non-leased IT equipment in a legal, cost-effective manner.

6.2 Scope

This policy applies to the proper disposal of all non-leased Tooele County IT hardware, including PCs, printers, handheld devices, servers, hubs, switches, bridges, routers, and so on. Any equipment considered no longer useful due to end-of-life, product life cycle, surplus, or obsolete condition, and any equipment beyond reasonable repair or reuse, are covered by this policy.

6.3 Policy

6.3.1 Asset Disposal

Legal Requirements - Tooele County's surplus or obsolete IT assets and resources (for example, desktop computers, laptops, servers, tablets, etc.) must be discarded according to legal requirements and environmental regulations through the appropriate external agents and following Tooele County's upgrade guidelines. Therefore, all disposal procedures for retired IT assets must adhere to county-approved methods.

Responsibilities - It is the responsibility of any employee of Tooele County's Information Technology Department with the appropriate authority to ensure that IT assets, equipment, and hardware are disposed of according to one or more of the methods defined below. It is imperative that any disposals performed by Tooele County are done appropriately, responsibly, and ethically, as well as with county resource planning in mind.

Obsolete IT Assets - Identifying and classifying IT assets as obsolete is the sole province of the Information Technology Department. Decisions on this matter will be made according to Tooele County's purchasing/procurement strategies. Equipment lifecycles are to be determined by IT asset management best practices (for example, total cost of ownership, required upgrades, etc.).

Reassignment of Retired Assets - Reassignment of computer hardware to a less-critical role is made at the discretion of the Information Technology Department, Department Head and/or Elected Official. However, it is the goal of Tooele County – whenever possible – to reassign IT assets to another business function to achieve full return on investment (ROI) from the equipment and to minimize hardware expenditures.

Trade-Ins - Where applicable, when a piece of equipment is due for replacement by a newer model, a fair market trade-in value should be obtained for the old IT asset by reselling, auctioning, donating, or reassigning the asset to a less-critical function. Tooele County's Information Technology Department will assume this responsibility.

Income Derived from Disposal - All receipts from the sale of IT assets must be kept and submitted to the Tooele County Treasurer's Office. Income derived from sales to the public,

or through online auctioning must be fully receipted and monies sent to the Tooele County Treasurer's Office. Sales to staff should be advertised through online auctioning.

Cannibalization and Assets Beyond Reasonable Repair - The Information Technology Department is responsible for verifying and classifying any IT assets beyond reasonable repair. Where possible, this type of equipment should be cannibalized for any spare and/or working parts that can still be used within the organization. The Information Technology Department will inventory and stockpile these parts as needed. Remaining parts and/or whole machines unfit for use or any other disposal means will be sent to an approved scrap dealer or salvaging company.

Sanitization of Assets - All hardware slated for disposal by any means must be fully wiped clean of all county data. Tooele County's Information Technology Department will assume responsibility for sanitizing this equipment by deleting all files, county-licensed programs, and applications according to the requirements in the Information Technology Hardware Sanitization Policy. In addition, any property tags or identifying labels must also be removed from the retired equipment.

Hazardous Materials - Hazardous materials such as lead, mercury, bromine, cadmium, etc. must be thoroughly removed from computer hardware before shipment to a landfill. The Information Technology Department may perform this action using government-approved disposal methods or hire an accredited disposal company specializing in this service. In either case the removal and discarding of toxins from Tooele County equipment must be in full compliance with local and federal laws.

Donations - IT assets that are not assigned for reuse, discard, or external buyers may be donated to a county-approved school, charity, or other non-profit organization (for example, a distributor of free machines to developing nations). All donations must be authorized by Tooele County Management. All donation receipts must be submitted to the Tooele County Auditor's Office for taxation purposes.

6.4 Related Documents:

Asset Management Policy

Hardware Sanitization Policy

IS-07 – Hardware Sanitization Policy

7.1 Purpose

This policy defines the standards and procedures for sanitizing Tooele County IT hardware before disposal in order to protect Tooele County intellectual property and maintain the confidentiality of PII or PHI or other sensitive information.

7.2 Scope

This policy applies to all hardware owned or leased by Tooele County that is capable of storing Tooele County's intellectual property or information related to the privacy of Tooele County's employees, clients, or suppliers. This policy applies to, but is not limited to, workstations and portable and notebook computers running Windows, UNIX, Linux, or Mac OS operating systems.

7.3 Policy

7.3.1 Requirements

Prior Approval - The Information Technology Department must be consulted prior to disposing of any computer equipment. The Information Technology Department Helpdesk is the primary contact for sanitization issues. The Helpdesk will use an approved sanitization tool and will aid in properly sanitizing the hardware.

Certification - The Information Technology Department Helpdesk or their designee must sign a certification that the equipment has been properly sanitized before it can be made surplus, transferred, or donated. Copies of all certification statements should be maintained by the Information Technology Department.

Other Devices - The following devices and storage media are not specifically addressed by the terms of this policy, but must be sanitized accordingly:

a. Servers should be backed up and sanitized in accordance with vendor recommendations. If the vendor has not provided recommendations, servers can be sanitized as workstations.

b. Removable storage media such as flash memory devices, floppy disks, optical CD and DVD media, tape, and other long-term storage media must be destroyed by incineration, shredding, or melting prior to disposal.

7.3.2 Scenarios for Disposal

Disposal Categories - Tooele County recognizes two different categories for the disposal of hardware:

a. **Hardware Transferred Internally** - Hardware may not require sanitization if it is transferred to another user within the same department. Hardware that is either transferred to a different department or to an employee with less authority must be sanitized as hardware transferred externally.

b. **Hardware Transferred Externally** - All hardware transferred externally must be sanitized according to the methods defined in this policy. This includes the following situations:

   1. Hardware donated to charitable organizations.
   2. Hardware returned to a leaser.
   3. Hardware returned to a vendor for servicing or maintenance.
   4. Hardware released to an external agency for disposal.

7.3.3 Technical Guidance on Sanitization

Sanitization Methods - Two different methods may be used to sanitize hardware:

a. **Physical Destruction** - Hardware may be sanitized through crushing, shredding, incineration, or melting.

b. **Digital Sanitization** - Simple deletion of files is insufficient to sanitize hardware. A digital sanitization tool must be used. The tool must conform to one of the following standards:

   1. RCMP TSSIT OPS-II (Royal Canadian Mounted Police Technical Security Standards for Information Technology, Appendix OPS-II).
   2. DoD 5220-22.M.
   3. The Gutman Wipe.
   4. Pseudo Number Random Generator PRNG Stream with eight passes.

7.4 Related Documents

Asset Management Policy

Asset Disposal Policy

IS-08 – Mobile Computing Security Policy

8.1 Purpose

This policy defines the information security requirements for the protection of sensitive Tooele County information on all mobile and portable computing devices.

8.2 Scope

This policy applies to all users who handle or are assigned tangible mobile computing, communications, or information assets belonging to Tooele County, including all employees, contractors, partners, or temporary personnel. It also applies to any personally owned mobile devices that are permitted to access Tooele County information assets.

8.3 Policy

8.3.1 Mobile Device Configuration

Approved Mobile Devices –Any Tooele County owned mobile device is authorized to be used for county business purposes. Non-county owned devices to be used for county business must have written authorization from the Tooele County Information Technology Director. Non-county devices may be used without authorization for VMWare Horizon client.

Security Configuration - Mobile computing devices such as laptops, tablets, or smart phones must be configured with approved security controls before being used to access or store Tooele County business information. Mobile devices must have encryption enabled.

Strong Passwords - All portable devices used for Tooele County business purposes must have a strong password or PIN enabled. Passwords must conform to the Tooele County Password Standard.

Approved Software or Applications - Only approved applications or software may be installed on mobile devices owned by Tooele County and used for business purposes.

Storage Media and Portable Memory - Portable data storage media and memory devices such as flash drives must be encrypted and protected with approved security controls.

Patches and Updates - Devices must be kept up to date by installing new patches or updates. Users should check regularly for updates and apply them promptly, within two weeks of release at a minimum.

Jailbreaking or Rooting - Users are prohibited from jailbreaking or rooting mobile devices or installing any software or firmware designed to bypass device security. Can only be monitored with EDM Software.

8.3.2 Enterprise Device Management (EDM)

Sensitive Data on Mobile Devices - Employees must not store or process Restricted Tooele County information on mobile devices. Only Internal Use Tooele County information

appropriate for the normal business activities of the individual user may be stored or used on approved mobile devices.

EDM Software - The Information Technology Department may install EDM software on any mobile device used for business purposes to manage security configuration of the device and protect Tooele County information.

EDM Controls - EDM software will enable the Information Technology Department to manage updates, remotely wipe, track location, or remotely lock mobile devices.

Decommissioning or Disposal - All Tooele County mobile devices will have hard drives removed before decommissioning or disposal.

Public Internet - Users are prohibited from using public Internet access or unsecured network connections while using mobile devices for work purposes.

8.3.3 Physical Protection

Protection of Mobile Devices - Employees must ensure the physical security of mobile computing devices and must protect them from damage or loss. For example, laptop computers should never be placed in checked airplane luggage or left in an unattended vehicle, unless secured in an out of site location. This policy excludes TCSO vehicles that require laptops that are physically mounted in the vehicle.

Reporting Lost or Stolen Devices - All Tooele County users must report lost or stolen mobile devices to the Information Technology Department within 24 hours.

8.4 Related Documents

Asset Management Policy

Acceptable Use Policy

IS-09 – Physical Security Policy

9.1 Purpose

This policy establishes the requirements for managing physical access to Tooele County buildings and facilities.

9.2 Scope

This policy applies to all offices and computer processing facilities operated by Tooele County. It applies to all employees and visitors to Tooele County buildings and facilities.

9.3 Policy

9.3.1 Security of Buildings and Facilities

Controlled Entry - Tooele County office facilities and data centers must have clearly defined security boundaries and must be protected with appropriate barriers and methods for controlling entry.

Security Tiers - Three tiers of security are provided for Tooele County buildings and facilities:

a. **Public:** Areas accessible by visitors prior to checking in, such as foyers, reception areas, elevators, public offices, and parking facilities.

b. **Secure:** Controlled areas for general employee access, for example, offices, cubicles, conference rooms, break rooms, areas behind reception desks, and other locations consistent with day to day business operations.

c. **Restricted:** Very secure areas controlled with additional layers of security, for example, data centers, computer rooms, telecommunications closets, and other areas accessible only by those with proper authorization.

Physical Access Monitoring - Video cameras or other access control mechanisms that monitor the entry and exit points to secure areas must be in place and must be protected from being tampered with or disabled.

9.3.2 Access Badges

ID Badges - Workers must display their Tooele County official-issued ID badges at all times when in Tooele County access-controlled buildings or facilities. Workers must never use another person's badge or loan their badge to someone else.

Temporary Badges - Workers who forget their ID badge must obtain a temporary badge by providing a driver's license or other picture ID.

ID Badge Control System - Tooele County must implement a system to manage the issue, modification, and revoking of ID badges.

Access Control - Workers must scan their own badges at badge readers to enter controlled-access areas. Workers must not allow other individuals to enter at the same time (tailgating) without scanning their own badges unless they are escorted visitors.

Individuals Not Displaying ID Badges - Individuals in controlled-access areas not displaying an official ID badge should be stopped and questioned. If they cannot produce a valid badge, they must be escorted to the reception desk. If such individuals behave in a threatening manner, workers must contact the Sherriff's Office immediately.

Security of ID Badges - Workers must protect ID badges from loss. Lost or stolen badges, including visitor badges, must be reported immediately to the IT Help Desk.

9.3.3 Visitors

Visitor Access - Visitors to Tooele County IT Department must check in at the IT front desk and show a picture ID.

Visitor Log - All visitors must sign the visitors log and provide their name, company they represent (if applicable), time arrived, individual visited, and time departed.

Visitor Badges - Visitors must wear a visitor badge and be escorted at all times while on Tooele County premises. Badges must be surrendered at the end of the visit.

9.3.4 Data Centers

Data Center Environment - All information systems must be housed in a Restricted security environment. Servers and other network infrastructure must never be installed in locations that do not have physical access controls.

Wireless Networks - Wireless networks are prohibited in Tooele County data centers.

Emergencies - In the event of an emergency, security control procedures will be suspended to the extent necessary to guarantee the physical safety of workers. Human safety must always supersede security requirements.

Access Control - Access to data centers must be limited to personnel directly associated with the use, maintenance, and support of these facilities. There are two levels of access:

a. **General Access** - Given to authorized individuals who need free access into the data center in order to carry out assigned duties. Requests for General access must be submitted to the IT Department by the employee's manager or supervisor along with supporting justification.

b. **Escorted Access** - Closely monitored access given to individuals who have a legitimate business need for occasional or special access. Escorted individuals must sign in and out and must be accompanied at all times by an individual with General Access. Requests for Escorted Access must be submitted to and approved by the Information Technology Department. Access by visitors, vendors, or other personnel will be considered on a case-by-case basis.

Data Center Doors - All data center doors must remain locked at all times and may only be temporarily opened to allow entry and exit of authorized individuals or permit the transfer of supplies or equipment.

Air Cooling Failure - In the event of an air-cooling system failure, a door to the data center may be temporarily propped open if it becomes necessary to increase airflow. If this happens, access must be controlled by remote monitoring or in person by an individual with General Access.

Deliveries - All deliveries to a data center require prior notification and approval. Delivery and receiving facilities must maintain required security controls.

Unauthorized Entry - The Information Technology Department must be notified immediately if an unauthorized individual is found in the data center. The unauthorized individual should be escorted from the data center unless there is the possibility of threat or danger. If so, law enforcement should be notified immediately. An incident report must be submitted to the Information Technology Director.

Access Termination - Access will be revoked whenever employment is terminated, job responsibilities change so that access is no longer required, or a worker fails to comply with security or data center policies and procedures.

IS-10 – Firewall Management Policy

10.1 Purpose

This policy defines the essential rules for protecting, managing, and maintaining all Tooele County firewalls.

10.2 Scope

This policy applies to all Tooele County firewalls, as well as any systems performing the role of firewalls, such as routers, air gaps, telecommunications front-ends, or gateways.

10.3 Policy

10.3.1 Requirements

Firewalls - Tooele County network assets must be protected by appropriately configured firewalls or systems performing the role of firewalls.

Paths and Services - The Information Security Committee will only approve firewall paths and services with a justifiable business need, and only if required security measures are in place. Any changes to existing paths or services must go through the same approval process.

Exceptions - All exceptions to standard firewall deployment and configuration must be approved in advance and in writing.

Documentation - Prior to deploying any firewall, a description of not permitted services and a network diagram must be submitted to the Information Security Committee.

10.3.2 Implementation and Operation

External Connections - All Internet connections to and from Tooele County internal networks must be protected by a firewall.

Sensitive Information on Secured Subnets - Portions of the internal network containing sensitive information must reside on a secured subnet with restricted access.

Demilitarized Zone (DMZ) - All Internet facing servers must be located within a DMZ, a subnet separated from the both the Internet and internal networks by one or more firewalls.

Default to Denial - All paths and services not specifically permitted are blocked by default.

Firewall Access Privileges - Access to modify firewalls is restricted to authorized personnel.

Firewall Physical Security - Firewalls not housed in a data center must be kept in locked rooms, closets, or cabinets that meet Tooele County physical security standards and must be accessible only to authorized personnel.

Application Firewalls - An application firewall must be configured and placed in front of all externally facing web applications.

Intrusion Detection and Prevention - All firewalls must be monitored by at least one form of intrusion detection or prevention.

Firewall Logs - All firewalls must log any suspicious activity, or changes to firewall configuration parameters, services, or connectivity paths. Logs must be protected by checksums, digital signatures, and/or encryption, and must be periodically reviewed. The logs will be retained for 1 year.

Testing - Firewalls must be tested periodically to ensure proper operation and configuration are maintained.

10.3.3 Change Management

Patches and Updates - Firewall administrators will install and run software patches and updates as recommended by the vendor. All other updates must be reviewed and approved by authorized personnel.

Changes to Rule Sets - All change requests will be evaluated against current Tooele County information security policy. All requests for changes to a firewall rule-set must include:

- **a.** source address(es), including IP's and domain names (where applicable).
- **b.** destination address(es), including IP's and domain names (where applicable).
- **c.** port(s) and or app(s) requested to be open.
- **d.** date of the change.
- **e.** point of contact.
- **f.** department name.

Changes to URL Filtering - All change requests will be evaluated against current Tooele County information security policy. All requests for changes to URL filtering must include:

- **a.** the URLs or URL categories to be unblocked.
- **b.** date of the change.
- **c.** point of contact.
- **d.** department name.

Emergency Changes - Emergency change requests must be approved by authorized personnel.

IS-11 – Information Classification and Handling Policy

11.1 Purpose

This policy describes the information classification and secure handling requirements for Tooele County information assets.

11.2 Scope

This policy applies to all Tooele County computer systems and data, and all users with access to Tooele County information assets.

11.3 Policy

11.3.1 Roles and Responsibilities

Classification Authority - The Tooele County Information Technology Department (or Information Owner) oversees the classification and labeling of all Tooele County information resources.

Information Owner - All production information must have a designated Information Owner responsible for ensuring the necessary controls are in place to assure confidentiality, integrity, and availability of the information. Information Owners will also ensure that all Tooele County data under their control is properly destroyed according to this policy when no longer needed.

Information Custodian - The Information Custodian will supervise the proper maintenance and control of Tooele County information according to the Information Owner's instructions.

Information Users - Users must access only those information assets they are entitled to, as required by job duties. Users must handle information securely and protect it from compromise.

11.3.2 Information Classification

Classification Labels - The Information Technology Department will assign all Tooele County information resources with an appropriate classification. Each classification must include distinct handling, labeling, and review procedures.

Classification Descriptions - Information and electronic data will be classified into one of four categories. The following list describes each category, in order of increasing confidentiality:

a. **PUBLIC** - Information formally approved for public release that may be disseminated without potential harm. By definition, there is no such thing as unauthorized disclosure of this information, but it must be protected at its official source from loss or change. Examples include product and service brochures, advertisements, job opening announcements, and press releases.

b. **INTERNAL USE** - Information generally accessible within Tooele County but not intended for entities or persons outside the organization. The default classification

when no higher confidentiality requirements exist. May have additional handling or access control requirements. Unauthorized disclosure is against policy but should not adversely impact Tooele County or its users, suppliers, business partners, or customers. Includes most e-mail, other correspondence, and documents; organization charts; work e-mail addresses and telephone numbers; and most software.

c. **CONFIDENTIAL** - Any information about or possessed by Tooele County that is more sensitive than most Internal Use data, but not to the level of Restricted data, requires special handling and controls that limit access and use. Unauthorized disclosure could adversely impact Tooele County or its constituents, contractors, suppliers, business partners, or users. Including most personal information (such as salary and performance evaluations), organizational plans or strategies not yet announced, most organization financial information, customer transaction data, computer passwords, and internal audit reports. For purposes of this policy, Confidential Information should be broadly construed.

d. **RESTRICTED** - Information with the highest degree of sensitivity where confidentiality, integrity, and regulatory compliance needs are very high and a failure in protection could have severe consequences for Tooele County and its customers, business partners, and suppliers. Requires the strictest rules of handling and usage. Examples include a person's name in association with Social Security Numbers or Tax ID, government identifiers, aggregated financial information, and protected health information (PHI). It also includes computer passwords, encryption keys, physical security information, and other regulated information Tooele County has a duty to protect.

Privacy Classification Categories - Personal information is classified into one of the following three categories:

- ***Personal Identifiable Information (PII)*** - Information used to identify an individual as different from any other person. Includes name, age, and date of birth; marital status; gender; street address; email address; citizenship; nationality; languages spoken; and telephone number.
- ***Sensitive Personal Information (SPI)*** - Information requiring additional privacy and security safeguards relating to the collection, consent, processing, use, storage, disclosure, and disposal of such information. Includes, but is not limited to, financial information, credit card information, bank account numbers, driver's license numbers, social security or national identity numbers, passport numbers, religious or philosophical beliefs, racial or ethnic origin, trade-union membership, political opinions, data concerning health and health related information, sex life, data relating to offenses or criminal convictions, and biometric personal information.
- ***Personal Health Information (PHI)*** - Sensitive details about a patient, such as medical conditions and health insurance claims that a healthcare professional collects to identify an individual and determine appropriate care. Includes birthdate, demographic information, medical histories, test and laboratory results, mental health conditions, insurance information, and other medical data.

Default Classification - Information without a label is classified by default as Internal Use.

Classification Changes - The Information Technology Department (or Information Owner) may at any time change the classification of certain information. When this occurs, the

classification label must be changed, and notification sent to all known recipients and custodians.

Information Handling - See the Appendix - Information Handling Requirements.

11.3.3 Electronic Data Destruction

Information Security Standards - The Information Owner or Custodian will specify standards for the proper destruction of information assets.

Hard Drive Removal - Before disposal, the IT Department must remove the hard drives from all servers, computers, and laptops and properly destroy them.

11.3.4 Disposal of Hardcopy Documents

Secure Information Containers - Hardcopy documents with Restricted, Confidential, or Internal Use information must be placed in one of the locked destruction containers located in Tooele County offices so it can be shredded. It must never be placed in trash or recycle bins or left in other publicly-accessible areas.

IS-12 – Backup and Recovery Policy

12.1 Purpose

This policy defines the requirements for creating, maintaining, storing, and recovering backup copies of information processed or stored on Tooele County computer and communications systems.

12.2 Scope

This policy applies to all Tooele County computer systems and data.

12.3 Policy

12.3.1 Backup Types and Schedules

Full Backups - Full backups for all file servers, shares, home drives, critical data, and databases will be performed as needed.

Differential Backups - Differential backups will be performed daily between 5 pm and 6 am.

12.3.2 Retention and Storage

On-site and Off-site Storage - All backups will be stored both locally and off-site on a daily basis.

Retention Periods - Backups are continuous and can be retained for up to 1 year.

Onsite Storage - Onsite backups must be kept on the Storage Area Network (SAN) in the Tooele County data center in an environmentally protected and access-controlled location. Backup drives must be kept physically and logically separate from drives storing production data.

Offsite Storage - Offsite storage of backup data must be kept in an environmentally protected site that is a sufficient distance away from the originating corporate facility to not be affected by a disaster or other event that impacts onsite data storage. Physical access must be controlled and authorized.

Cloud Storage Backups - Only those cloud services officially approved by Tooele County will be used to store or back up data.

Backup Encryption - All backups of sensitive, valuable, or critical information must be encrypted.

No Backups of User Devices - Users must store all Tooele County information on assigned drives and directories where it can be backed up.

Email Backups - Email system backups are performed by an approved service provider and will be retained for a minimum of 3 years and up to 99 years.

12.3.3 Testing and Review

Backup Recovery Testing - Backups must be tested at least semi-annually to provide assurance that critical business information and software can be fully recovered.

Location and Storage Media Review - Each location used to store Tooele County backups must be reviewed at least annually to determine that backups and storage systems are secure.

12.4 Related Documents

Business Continuity Policy

IS-13 – Third-Party Risk Management Policy

13.1 Purpose

This policy defines the requirements for selection and oversight of third parties that access, store, process, or transmit Tooele County data in the course of providing services to Tooele County.

13.2 Scope

This policy applies to all third-party users who have access to Tooele County internal information resources and data.

13.3 Policy

13.3.1 Vendor Selection

Needs Analysis - Before selecting a vendor, Tooele County must prepare an analysis of what is needed and assess how engaging a third party is the preferred course of action. Once the need for a third-party solution has been confirmed, a reasonably broad range of vendors should be surveyed before making a final choice of candidates.

Risk Assessment - An assessment of third-party candidates may be conducted and consider the following risk factors as appropriate:

- **a.** Audited financial statements, annual reports, SEC filings, and other available financial indicators.
- **b.** Significance of the proposed contract on the third party's financial condition.
- **c.** Experience and ability in implementing and monitoring the proposed activity.
- **d.** Business reputation.
- **e.** Qualifications and experience of the company's principals.
- **f.** Strategies and goals, including service philosophies, quality initiatives, efficiency improvements, and employment policies.
- **g.** Existence of any significant complaints or litigation, or regulatory actions against the company.
- **h.** Ability to perform the proposed functions using current systems or the need to make additional investment.
- **i.** Use of other parties or subcontractors by the third party.
- **j.** Scope of internal controls, systems and data security, privacy protections, audit coverage, audit attestation reports, or other certifications.
- **k.** Business resumption strategy and contingency plans.
- **l.** Knowledge of relevant consumer protection and civil rights laws and regulations.
- **m.** Adequacy of management information systems.
- **n.** Adequacy of information security posture.

o. Insurance coverage.

13.3.2 Vendor Contracts

Nondisclosure Agreements - Before being given access to Tooele County information assets, all third-party individuals must sign nondisclosure agreements regarding the sharing of any internal or sensitive information.

Contract Oversight - The contracting process between Tooele County and the third-party service provider must be overseen by the primary consuming department and may have oversite from the Tooele County Information Security Committee, who will ensure contractual requirements are fulfilled regarding security responsibilities, controls, and reporting.

Performance Oversight - Third-party relationships and performance will be managed by the primary consuming department and the Tooele County Information Security Committee. These groups will:

a. Evaluate the overall effectiveness of the third-party relationship and the consistency of the relationship with Tooele County strategic goals.

b. Review any licensing or registrations to ensure the third party can legally perform its services.

c. Ensure appropriate security processes and controls are being followed to protect Tooele County information assets.

d. Evaluate the third party's financial condition at least annually. Audited financial statements should be required for significant third-party relationships.

e. Review the adequacy of the third party's insurance coverage.

f. Ensure that the third party's financial obligations to others are being met.

g. Review audit reports or other reports such as a SOC 2, Type 2 report provided by the third party, and follow up on any needed corrective actions.

h. Monitor for compliance with applicable laws, rules, and regulations.

i. Review the third party's business resumption contingency planning and testing.

j. Assess the effect of any changes in key third party personnel involved in the relationship with Tooele County.

k. Review reports relating to the third party's performance in the context of contractual requirements and performance standards, with appropriate follow-up as needed.

l. Review customer complaints about the products and services provided by the third party and the resolution of the complaints.

m. Meet as needed with representatives of the third party to discuss performance and operational issues.

Incident Management - The Tooele County Information Security Committee will coordinate security incident response policies and contractual notification requirements with the third-party.

IS-14 – Vulnerability and Patch Management Policy

14.1 Purpose

This policy defines the requirements for the detection and mitigation of host and server operating system and application vulnerabilities, including the management of patches and updates, excluding custom software applications.

14.2 Scope

This policy applies to all users of Tooele County computer systems and assets. Secure development operations and application source code scanning are excluded from the scope of this policy.

14.3 Policy

14.3.1 Network Inventory

Scan Tool Updates – The Information Technology Director or assigned personnel will ensure that the vulnerability scanning tool is regularly updated with new security vulnerabilities.

Network Inventory Maintenance - The Senior Network Specialist will maintain an inventory of all internal and external network segments and interfaces.

Inventory Updates - All new network segments and public facing systems will be entered into the vulnerability scanning tool once they are approved and implemented by the Senior Network Specialist.

Internal Network Segments - The list of internal network segments will be reconciled between the network inventory and the vulnerability scanning tool at least every 6 months.

14.3.2 Internal Vulnerability Scans

Authenticated Scans - All internal vulnerability scans must run in authenticated mode (credentialed scans), either remotely with an administrator account, or using an agent.

Scanning Credentials - The account used for authenticated (credentialed) scans must only be used for that purpose.

Scan Tool Access - Only authorized users are allowed access the vulnerability scanning tool.

Authenticated Scanning Exceptions - Where authenticated vulnerability scanning is not feasible or practical, unauthenticated scans may be run every 90 days, with a local authenticated scan performed at least once every 90 days.

Network Segments - All network segments must be scanned at least every 90 days.

14.3.3 External Vulnerability Scans

Public Facing Systems - All public facing systems must be scanned at least every 90 days.

External Web Apps - All external web apps managed by Tooele County must be subject to an annual penetration test that includes a web app vulnerability scan.

Third Party Systems - Systems hosted by a third party may be excluded from external scanning provided there are sufficient contract provisions addressing vulnerability management.

14.3.4 Vulnerability Remediation

Scan Configuration - Where possible, scans must be run with all available plugins.

Critical Vulnerabilities List - A prioritized list of all high and critical vulnerabilities must be delivered to the Information Technology Director for remediation.

Disruptions - Security updates and patches must be carefully coordinated to avoid causing unexpected system outages or disruptions.

Patching Frequency - Based on the criticality of identified vulnerabilities, patching must be accomplished within the following time limits:

a. **Critical Vulnerabilities** - Must be remediated within 7 business days.

b. **High-risk Vulnerabilities** - Must be remediated within 30 days. Where possible, external vulnerabilities should be addressed sooner.

c. **Non-critical Vulnerabilities** - Medium, Low, and Informational vulnerabilities will be addressed during the 30-day patch cycle. Non-security updates may be planned and deployed on a case by case basis.

Compensating Controls - When circumstances prevent patching a critical or high-risk vulnerability, compensating controls must be implemented to mitigate the risk. All compensating controls must be approved by the Tooele County Information Security Committee.

Patch Testing - Before being deployed in production systems, critical patches should first be deployed and tested in environments where a degradation or outage will not cause significant impact.

Legacy Software Risk - A risk assessment should be conducted for older software that can no longer be updated or is no longer supported by the vendor. Vulnerability risks of legacy software must be weighed against operational needs, and a decision made by the Information Security Committee whether to retire an application, replace it, or accept the business risk.

IS-15 – Information Security Awareness Policy

15.1 Purpose

This policy defines the requirements for creating and managing the Tooele County Information Security Awareness Program. The program will be designed to teach good security practices and behaviors and measure improvement over time.

15.2 Scope

This policy applies to all employees, contractors, partners, and third-parties with access to Tooele County information assets.

15.3 Policy

15.3.1 Roles and Responsibilities

Tooele County Management - Establishes and supports the Information Security Awareness Program as an integral part of the greater Information Security Program.

Information Technology Director - Establishes the requirements for Information Security Awareness training, including frequency of training, training concepts, delivery methods, and measurement.

Information Technology Department - Manages the delivery of information security awareness training and tracks completion. Maintains Awareness training records.

Department Heads and Elected Officials - Ensure that All users complete the appropriate information security training and follow required information security behaviors and best practices.

15.3.2 Requirements

Information Security Training - All employees with access to Tooele County information systems and data must complete the basic information security training course when hired within 14 days and must repeat the training semi-annually. Additional training may be required when job duties change or as the result of a policy violation.

Types of Training - Training will be delivered by one or more of the following methods:

a. Online courses

b. Periodic Phishing tests

c. Supplemental materials such as surveys, posters, videos, newsletters, or other similar resources

Measurement/Metrics - The Awareness program will include a system to measure user compliance and improvement.

Enrollment Notification - Individuals will be notified by e-mail within 24 hours of enrollment in an awareness training course. Individuals who have not completed the training within 7 days will receive e-mail reminders.

Department Heads and Elected Officials Notification - Will be notified by e-mail of individuals under their supervision who do not complete the course within 30 days.

Enforcement - Workers who fail to complete assigned cybersecurity training will lose access to Tooele County information systems until they have completed training.

IS-16 – Secure Application Development Policy

16.1 Purpose

This policy establishes the security requirements for Tooele County application development work.

16.2 Scope

This policy applies to all individuals with a role in Tooele County application development and approval.

16.3 Policy

16.3.1 Secure Application Development

Security Requirements - All internally developed software products must meet the appropriate information security requirements defined by the Information Security Committee.

Information Leakage - Code must be configured and compiled with rules that prevent information leakage at runtime. For example, application error messages must not reveal information about application architecture or the Tooele County network.

Standardized Framework - All development work must take place within a standardized framework for secure application development that integrates current industry best practices and standards such as the following:

a. **SEI CERT** - Secure coding standards for application development

b. **OWASP** - Secure coding standards for web-based applications

Security Impact Review - A Security Impact Review must be completed at each stage of development. All findings must be addressed before production migration.

Developer Training - All application developers must be properly trained in secure coding standards and techniques.

Separation of Environments - Appropriate controls must be in place to ensure physical and logical separation of development, test, and production environments.

Test Environments - Test environments must emulate the production environment as closely as possible, including the use of a common operating system, database, web application server, and similar hardware.

16.3.2 Code Management

Source Code Library - A library of previous source code versions must be maintained, along with configurations, parameters, procedures, and other supporting documentation.

Application Source Code - Source code must not be stored on production systems. Environments containing application source code must be configured to prevent unauthorized access.

16.3.3 Production Data in Test Environments

Approval - Any unaltered production data used for test purposes in non-production environments must be approved by Information Owners and Information Technology Director.

Data Control - If production data is copied to a test system, the data must be given a similar level of control as in the production system.

Test Data Removal - Test data, test accounts, custom application accounts, user ID's and/or passwords must be removed before a system is activated in production.

16.3.4 Code Changes

Updates and Patches - All software releases, patches, and updates to production systems must to be tested for functionality and security prior to installation in production.

Code Review - Code changes must be reviewed by someone (not the code author) who is trained in proper code review techniques and secure coding practices. An approved automated code review tool may also be used for testing. Based on the results, appropriate corrections must be made, and the changes reviewed and approved by management prior to release.

Changes During Acceptance Testing - Developers must not make changes to code during acceptance testing. If changes are necessary, the developer must make modifications in the development environment and submit the changed code for retesting.

16.3.5 Default Settings

System Default Settings - System default settings that could potentially compromise security must be changed before a system is placed into a production environment.

Default Passwords - All default passwords must be changed prior to a system being placed in a production environment.

IS-17 – Charter: Information Security Committee

17.1 Purpose

This Information Security Committee (ISC) provides leadership in the protection of information assets and their data. The committee members advise on and prioritize the development of the information security initiatives, projects, and polices. The county acknowledges the critical, ongoing need to provide a comprehensive oversight process designed to protect its information assets and electronic systems from internal or external threats and harm. The ISC is charged to coordinate and direct the development of appropriate cyber policy to address that need. The ISC will be advised regarding assessment activities and will provide advice regarding education and communication that may be needed to support the policy and compliance measures developed. The ISC will suggest resources needed for the county to manage IT security. These will be balanced with what are reasonable and acceptable levels of risk to be assumed by the county.

17.2 Authority

County manager:

The ISC shall have full access to all county data, records, facilities and personnel of the county as deemed necessary or appropriate by the county manager.

17.3 Scope

This ISC provides guidance and leadership to maintain and improve the confidentiality, integrity, and availability of all data and information assets for Tooele County.

17.4 Composition

ISC members shall be appointed by the county council. The ISC will perform an annual review of membership and recommend changes after considering needs for continuity and expertise, as well as the need to encourage change and opportunities to participate. Administrative support will be provided by the Information Technology Department.

The ISC shall be composed of:

- The Information Technology Director
- An employee of the Information Technology Department with expertise in information technology security
- An employee of the Human Resources Department
- A county employee with expertise in county finances or accounting
- An at-large county employee or member of the public

17.5 Committee Responsibilities

1. Data Governance – To provide oversight of policies, procedures, plans and execution intended to provide security, confidentiality, availability and integrity of the county's data and information systems.

2. Information Technology Systems – To oversee the quality and effectiveness of the county's policies and procedures with respect to its information technology systems, including privacy, network security, and data security.
3. Incident Response – To review and provide oversight on the county's policies and procedures in preparation for responding to any cyber incidents.
4. Disaster Recovery – To review periodically with management the county's disaster recovery capabilities.
5. Compliance Risks & Internal Audits – To oversee the county's management of risks related to its information technology systems and processes, including privacy, network security, data security, and any internal/external audits of systems and processes.
6. IT/Security Budget – To oversee the county's information technology senior management team relating to budgetary priorities based, in part, on assessing risk associated with various perceived threats.
7. Advisory Role – To review the county's information technology strategy or programs relating to new technologies, applications, and systems.
8. General Authority – To perform such other function and to have such powers as may be necessary or appropriate in the efficient and lawful discharge of the foregoing.

17.6 Meeting Schedule

Meetings will be held on a monthly cadence taking place on the first Tuesday of the month in room 125 of the Tooele County IT department building located at 47 S Main St, Tooele, UT 84074. The time the meeting will commence will be at 10:00 am MST and will last for 2 hours till 12:00 pm MST or when the agenda action items have been exhausted. Meetings may be adjusted for government holidays and notification given to ISC members via email a week prior to a meeting occurring.

17.7 Decision Model

Decisions will be made through ISC member consensus. Disputes will be resolved by assigned chairman of the ISC committee.

17.8 Meeting Agenda

An agenda will be drafted by the committee chair with consultation from committee members, staff, and other stakeholders. The draft agenda will be distributed to committee members on the Monday preceding the meeting. Feedback will be incorporated into the final draft agenda, which will be presented for adoption at the committee meeting. A sample agenda could include plans to:

- Discuss open issues from previous meetings
- Discuss any internal security issues which have emerged since the previous meeting
- Discuss any new external security issues which have emerged since the previous meeting
- Prioritize the open list of security issues in the risk register
- Assign responsibility and timelines for remediating security issues located in the risk register

17.9 Attendance

All members of this committee are expected to actively participate. Regular attendance for meetings as well as involvement in special activities is important to satisfy the many responsibilities of this committee. Members are expected to RSVP to meeting notices. Due to the nature of the committee work, member consistency is critical. If members are unable to attend, proxy will not be recognized. Committee members may invite additional attendees to participate as is appropriate in relation to meeting agenda items for discussion.

17.10 Communication

Meeting notes and action items will be documented at each committee meeting. Following each meeting, the ISC administrative support staff will distribute the documents to the chair for review. The resulting document, and other materials, will be distributed to the committee members prior to the next meeting. During the next meeting the documents will be approved. Once approved, the documents will be posted to the county's internal intranet. The committee charter, meeting schedules, membership roster and other documents will also be posted to the intranet.

TOOELE COUNTY

Appendix A- Information Handling Requirements

Tooele County Information will be handled and protected according to the following principles:

	PUBLIC	INTERNAL USE	CONFIDENTIAL	RESTRICTED
Storage	No restrictions on electronic or physical storage for some information. Some types may require an access request before being made available.	No external web or FTP except through VPN or remote access. Reasonable precautions to restrict physical access.	Restricted access secure corporate file share or database. Physical copies stored in a locked container; restrict access to authorized individuals.	Restricted access secure corporate file share or database. Physical copies stored in a locked container; restrict access to authorized individuals.
Protection	No restrictions.	Password authentication.	Validated strong passwords or multifactor authentication.	Strong multi-factor authentication and encryption.
Access	Read - No restrictions. Update - Controlled by Information Owner.	Read and Update - Information Owner designates based on role.	Read and Update - Information Owner designates based on role.	Read and Update - Information Owner designates by individual.
Transmission	No restrictions.	Encrypted.	Encrypted.	Encrypted.
FAX	No restrictions.	Reasonable precautions to restrict access and confirm delivery.	Not permitted.	Not permitted.
Copy, Scan, or Print	No restrictions.	In-house copying preferred; shred or place spoils and overruns in secure waste. If outside copying is used, original should be returned to the company and spoils destroyed by the supplier.	In-house copying required; shred spoils and overruns.	In-house copying required; copies numbered; shred spoils and overruns.
Destruction/ Disposal	Any method.	Shred or place in secure waste.	Shred.	Shred.
Labeling	May be labeled as Public.	May be labeled as Internal Use.	Must be explicitly labeled as Confidential.	Must be explicitly labeled as Restricted.

TOOELE COUNTY

Appendix B – Glossary of Terms

Definitions:

Access Fob - Any type of electronic key.

Account (User ID or Username) - A unique string of characters assigned to a user to identify that person while accessing a computer system or network. A user commonly must enter both a user ID and a password during the logon process.

Authenticated Vulnerability Scanning - Vulnerability testing performed with the privileges of a logged-in (authenticated) user. Authenticated scans determine how secure a network is from an inside vantage point**.**

Backup - The process of making copies of files and programs to a separate storage system in order to make them available for recovery after data is lost, corrupted, deleted, or destroyed by a disaster.

Baselines - Detailed configuration requirements for specific technologies. Baseline requirements focus on settings, configurations, parameters, and deployment options for a particular platform, product, service, vendor, or technology. Standard build images often embody baseline requirements. Where practical, all instances of a particular technology should be deployed according to the baseline in order to reduce variation and complexity.

Beyond Reasonable Repair - All equipment needing repair or refurbishing and where the cost is likely to equal or exceed that of total replacement.

BOGON - An invalid IP packet on the public Internet with an IP address that falls within a range not currently assigned for use (as opposed to an address reserved for special use). A bogus IP address.

Business Continuity Plan (BCP) - A documented set of instructions or procedures describing how an organization's business functions will be sustained during and after a significant disruption.

Business Impact Analysis (BIA) - A management-level analysis identifying the impacts caused by loss of organization resources. The BIA measures the effect of initial resource loss and escalating losses over time, in order to provide reliable data for decision making about risk mitigation and continuity planning.

CIRT (Computer Incident Response Team) - A carefully selected and well-trained group of responders whose purpose is to promptly and correctly handle a security incident so that it can be quickly contained, investigated, and resolved.

Confidential Information (Sensitive Information) - Any Tooele County information that is not publicly known, including tangible and intangible information in all forms, such as information that is observed or orally delivered, or is in electronic form, or is written, or in other tangible form.

Criticality - The importance of keeping information available for purposes of business continuity or disaster recovery. Criticality classifications define the amount of time required to recover or restore information and make it available for use. In the event of a major disaster or widespread systems failure, criticality ratings reduce resource conflicts and significantly speed up the recovery process.

Custodians, Information - See Information Custodians.

Data Privacy - See Information Privacy.

Differential Backup - Backs up only the files that have changed since the last Full Backup. Usually runs once a day but may be run more often for critical data.

Disposal - The reselling, reassignment, recycling, donating, or throwing out of IT equipment through responsible, ethical, and environmentally sound means.

DMZ - Demilitarized Zone. A specific type of network zone that acts as a buffer between internal networks and outside public networks in order to prevent direct outside access to internal information.

Electronic Messaging System - Any device or application that will provide the capability of exchanging digital communication between two or more parties. Examples are electronic messaging, instant messaging, and text messaging.

External Vulnerability Scanning - Vulnerability testing performed from completely outside the network without login privileges. Mainly probes weaknesses in the network perimeter.

Full Backup - Backs up all files and programs. Usually runs once a week due to the amount of storage required. May also be done after a major system change.

Guidelines - Statements of best practices designed to achieve policy objectives where cost, desire for latitude, or business impact prevent a mandatory requirement. Guidelines influence decision making and should be followed despite the absence of a specific mandate. Likewise, Guidelines are meant to steer decision making where cost of compliance is prohibitive, formal enforcement measures are unnecessary, non-compliance yields low risk, or uniform requirements are impractical.

IANA - Internet Assigned Numbers Authority. The international body that assigns IP address spaces under authority from the Internet Engineering Task Force (IETF).

IDS (Intrusion Detection System) - A software utility that runs on the NTS. Is the engine that monitors network traffic and scans it to match threat signatures. Can identify malicious activity, log information about it, and report it.

Incident - An occurrence that threatens the confidentiality, integrity, or availability of an information system, or that violates security policies or procedures.

Incremental Backup - Backs up only the files that have changed since the last backup of any type. Each backup file is smaller than the files for other backup types,

but it generally takes longer to restore data because both the last Full backup and all Incremental backups must be restored for a full rebuild.

Information Asset – Any Tooele County data in any form, and the equipment used to manage, process, or store Tooele County that data, used in the course of executing business.

Information Custodians - Designated individuals in physical or logical possession of information owned by or entrusted to Tooele County. While Information Technology (IT) department staff are clearly Custodians, local system administrators are also Custodians. Whenever information is maintained only on a personal computer, the User is a Custodian. Custodians are required to maintain the security measures defined by information Owners.

Information Owners - Department managers, members of the top management team, or their delegates responsible for the acquisition, development, or maintenance of systems and applications that process Tooele County information. Owners are responsible for making sure information is stored in the correct location with appropriate access controls.

Information Privacy - The aspect of information technology that deals with the ability of an organization or individual to determine what data in a computer system can be shared with third parties. The right of an individual to have some control over how personal information is collected and used. Also known as data privacy.

Information Privacy Program - A documented set of plans, policies, and procedures that outline how an organization will protect the personal information of its customers and clients. As part of an overall privacy program, a privacy plan spells out how an organization will comply with laws and regulations regarding the security of privacy information.

Information Security (InfoSec) - A set of strategies for managing the processes, tools, and policies necessary to prevent, detect, document, and counter threats to digital and non-digital information, regardless of how it is formatted, or whether it is in transit, being processed, or at rest in storage.

Information Security Awareness - The extent to which every individual who potentially has access to Tooele County information understands the importance of information security, the consequences of a lack of information security, their individual responsibilities regarding information security, and is willing to act accordingly.

Information Security Awareness Program - A documented formal process to educate users about computer security, establish individual responsibility for the organization's security policies, and measure program effectiveness. A successful Awareness program encourages the adoption of safe and secure online behaviors at all times, both in and away from the work environment.

Information Security Breach - Unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal or non-public business information maintained by the Tooele County.

Information Security Program - A documented set of information security policies, procedures, guidelines, and standards designed to ensure the confidentiality, integrity, and availability of an organization's essential data, as well as client and customer information and protect it from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption.

Information User - Any individual who has been authorized to access Tooele County information systems or data. Users must understand and comply with all Tooele County information security policies, procedures, and standards.

Internal Vulnerability Scanning - Vulnerability testing performed from inside firewall(s) to identify real and potential vulnerabilities inside the network. May be performed with or without login privileges.

IPS (Intrusion Prevention System) - A software utility that provides protective services for a network. Can identify malicious activity, log information about it, report it, and attempt to block or stop it. Has in-line capability to block network activity.

Jailbreaking - On devices running iOS, the process of removing software restrictions put into place by Apple so the user can download apps not in the App Store, use themes, and install unsupported extensions. Does not allow full control of the operating system the way rooting does on an Android device.

Least Privilege - The principle that users should only be given the minimum privileges and capabilities needed to accomplish required work.

Malicious Code - Software or firmware intended to perform an unauthorized process that will adversely impact the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host.

Malware - A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim’s data, applications, or operating system or of otherwise annoying or disrupting the victim.

Mobile Devices - For purposes of this policy, mobile computing assets are defined as tablets, cell phones, handhelds, and all portable storage media, including flash drives, smart cards, or tokens.

Need-to-Know - The principle that users should only be allowed to access the specific information needed to accomplish required work.

Network Zone - An isolated network segment with a custom security configuration that controls data movement into and out of the zone.

Non-leased - All IT assets that are the sole property of Tooele County; that is, equipment that is not rented, leased, or borrowed from a third-party supplier or partner company.

Obsolete - All equipment that no longer meets required functionality.

Owners, Information - See Information Owners.

Partner - Any non-employee of Tooele County who regularly provides some form of service to Tooele County.

Password - An arbitrary string of characters used to authenticate the identity of a user when attempting to log in to an Tooele County information asset, to prevent unauthorized access to the account.

Patch Management - A process used to update the software, operating systems, and applications on an information asset in a logical manner. The purpose of a patch management system is to highlight, classify, and prioritize any missing patches on an asset.

PHI (Protected Health Information) - Any health data created, received, stored, or transmitted by HIPAA-covered entities and their business associates relating to the provision of healthcare, healthcare operations, and payment for healthcare services. Protected health information includes all individually identifiable health information, including demographic data, medical histories, test results, insurance information, and other information used to identify a patient or provide healthcare services or healthcare coverage. 'Protected' means the information is protected under the HIPAA Privacy Rule.

Personally Identifiable Information (PII) - Any data that could identify a specific individual, either by itself or when combined with other identifying elements, for example, name, social security or other national ID number, date and place of birth, address, etc. This includes designations used outside of the US such as "personal information" or the European Union "personal data" requirements.

Policies - Requirements that establish authority or accountability. They provide the boundaries for making business decisions. They have broad scope and apply to a wide audience, but do not specify implementation details.

Recovery Time Objective (RTO) - The maximum acceptable period of time a computer, system, network, or application can be down after a failure or disaster before being returned to service and the necessary backups restored, in order to avoid unacceptable business consequences.

Recovery Point Objective (RPO) - The maximum period of time for which the business can tolerate a loss of information because there is no backup, or the backup is unrecoverable. It can also be expressed as the maximum age of files that must be recovered from backup for normal operations to resume if a computer, system, or network goes down. The RPO determines the minimum frequency of backups. For example, if the RPO is one hour, backups must be made at least once per hour. If the RPO is five days (120 hours), then backups must be made every 120 hours or less.

Remediation - The process of removing or alleviating a security vulnerability by patching the vulnerable system, implementing configuration changes, turning off vulnerable services, or even blocking exploitation attempts with an Intrusion Prevention System (IPS) device.

Remote Access - The process of connecting to internal resources from an external source (for example, from home, a hotel, or any other public area).

Residual Risk - Residual risk is the threat that remains after all efforts to identify and eliminate risk have been made. The four basic ways of dealing with risk are to reduce it, avoid it, accept it, or transfer it. Since residual risk is unknown, many organizations choose to either accept residual risk or transfer it, for example, by purchasing insurance to transfer the risk to an insurance company.

RFC 1918 - The IETF document that specifies the IP version 4 (IPv4) address ranges reserved for use by private networks. RFC 1918 IP addresses are not publicly routable and fall within the following ranges: 10.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.31.255.255, and 192.168.0.0 – 192.168.255.255.

RFC 4193 - The IETF document that specifies the IP version 6 (IPv6) addresses reserved for use by private networks. RFC 4193 Unique Local Addresses (ULA) are intended to replace RFC 1918 IP addresses as IPv6 comes into general use.

Risk Management - As applied to information security, the process of continuously assessing vulnerabilities and threats to information assets and choosing and applying the appropriate protective controls. In a broader sense, the process of identifying, assessing, and controlling any threats to an organization's capital and earnings from a variety of sources, including financial uncertainty, legal liabilities, strategic management errors, accidents, and natural disasters.

Risk Management Program - The plans, processes, procedures, activities, and tools that support the identification, assessment, response, control, and reporting of risk.

Role-Based Access Control (RBAC) - A model for controlling access to resources where privileges are assigned by roles rather than by personal identity.

Rooting - On devices running the Android operating system, the process of removing all limitations imposed by the manufacturer. Grants the user complete control of the operating system, unlocks all device features, allows installation unauthorized software or even complete replacement of the operating system.

Sanitization - The secure overwriting or destruction of all information on any form of data storage hardware or media in such a manner that the information is totally unrecoverable.

Segregation/Separation of Duties (SOD) - A basic internal control to prevent or detect errors and irregularities by assigning responsibilities to separate individuals so that no single person is in a position to take fraudulent actions without detection.

Sensitive Information - Any Tooele County information not publicly known and not for public distribution, including tangible and intangible information in all forms, such as information observed, orally delivered, electronic form, written, or in other tangible form.

Special Privileges - Advanced access, capabilities, or authorities that are significantly greater than those available to the regular user, for example, Systems Administrator privileges.

Standards - Requirements similar to policies, but more focused in scope, specificity, or subject matter. A mandatory action or rule designed to support and conform to a policy. Standards typically establish a more detailed application of a policy, often focused on a specific technology domain. Standards will be carefully scoped to ensure business objectives are balanced with risk management. This may be done by applying requirements only to high-risk systems or high-risk business functions. Where such scoping occurs, the requirements serve as guidelines for systems and environments belonging to a lower risk classification.

Surplus - Still functional hardware that has been replaced by upgraded equipment or is superfluous to existing requirements.

Telecommuter - Users who access Tooele County information systems from home or a remote location as part of a regular work schedule for extended periods of time.

Unauthenticated Vulnerability Scanning - Vulnerability testing performed without access privileges, either from within the network (Internal) or from outside the network (External).

Unsecured Protected Health Information - Protected Health Information (PHI) that is not rendered inaccessible, unusable, unreadable, or indecipherable to unauthorized persons.

User - See Information User.

VIP - Virtual IP address. An IP address shared by a group of servers or domain names.

Vulnerability - Weakness in an information system, security procedure, internal control, or implementation that could be exploited by a threat source.

Vulnerability Management - A process that discovers assets on a network, categorizes the OS and applications on the assets, and reports the security vulnerabilities found on the scanned systems.

Appendix C – Revision History

Revision History

Version	Date	Description	Author
1.0	03/21/19	Original Version	Secuvant
1.1	11/23/2020	Combination of Policies & updates for annual review	Secuvant
1.2	02/16/2021	Final – Approved by Tooele County Council	Denise Lawrence
1.3	05/04/2021	Correction of Contradictory Provisions and Grammatical Errors	Denise Lawrence Colin Winchester