**TOOELE COUNTY**
**RESOLUTION 2021-16**

**A RESOLUTION AMENDING THE TOOELE COUNTY INFORMATION SECURITY PLAN DATED NOVEMBER 23, 2020**

**WHEREAS,** the Tooele County Council adopted the Tooele County Information Security Plan dated November 23, 2020 via Resolution 2021-07 on February 16, 2021; and

**WHEREAS,** the Information Security Plan as adopted contains some contradictory provisions and grammatical errors; and

**WHEREAS,** the Tooele County Council desires to correct those contradictory provisions and grammatical errors;

**NOW, THEREFORE, BE IT RESOLVED BY THE TOOELE COUNTY COUNCIL** that the attached provisions of the Tooele County Information Security Plan dated November 23, 2020 are hereby amended to read as attached hereto, which attachment is, by this reference, made a part hereof.

**EFFECTIVE DATE:** This resolution shall take effect immediately upon passage.

**DATED** this 4th day of May, 2021.

**ATTEST:**

Marilyn K. Gillette
MARILYN K. GILLETTE, Clerk

**TOOELE COUNTY COUNCIL:**

TOM TRIPP, Council Chair

(S E A L)

Council Member Hamner voted aye
Council Member Hoffmann voted absent
Council Member Thomas voted aye
Council Member Tripp voted aye
Council Member Wardle voted aye

**APPROVED AS TO FORM:**

Colin Winchester 05/11/2021

COLIN R. WINCHESTER
Deputy Tooele County Attorney

TOOELE COUNTY
INFORMATION SECURITY PLAN
November 23, 2020

## 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.

---

## 2.3 Policy

...

### 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.

---

## 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.

---

## 17.4 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.

TOOELE COUNTY
INFORMATION SECURITY PLAN
November 23, 2020

## 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 ~~organization-wide~~ county-wide information security policies, standards, guidelines, and procedures, in conjunction with the Tooele County ~~Management~~ manager and the Tooele County Attorney.

**Information Security ~~Management~~ Committee (ISC)** - ~~An Information Security Management Committee shall be composed of two (2) Information Technology personnel including the IT Director, two (2) volunteer Department Head or Elected Officials, and one (1) volunteer employee. The Information Security Management Committee~~ The ISC will meet monthly to review information security for Tooele County. The ~~committee~~ 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~~ 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.

---

## 2.3 Policy

...

### 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 ~~Information Security Management Committee~~ 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 ~~Tooele County~~ Information Technology Director.

---

## 17.2 Authority

~~Executive sponsor/s~~ County manager:

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

---

## 17.4 ~~Committee~~ Composition

~~ISC membership will be approved by the current body based upon the members seniority, role within the county, and qualifications they will bring to the committee.~~ ISC members shall be appointed by the county council. The ~~committee~~ 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 ~~applicable department~~ Information Technology Department. ~~Current county departments necessitating mandatory committee membership are as follows.~~

- ~~Internal Audit – To help define security metrics and validate compliance~~
- ~~IT & Security Staff~~
- ~~Human Resources – To facilitate communication with personnel or mange training~~
- ~~Legal – To provide regulatory and legal compliance insight~~
- ~~Finance/Accounting~~
- ~~Third-Party Security Advisory~~

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 ~~counties~~ county's data and information systems.
2. Information Technology Systems – To oversee the quality and effectiveness of the ~~counties~~ 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 ~~of the county~~ in preparation for responding to any cyber incidents.
4. Disaster Recovery – To review periodically with management the ~~counties~~ county's disaster recovery capabilities.
5. Compliance Risks & Internal Audits – To oversee the ~~counties~~ 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 ~~counties~~ 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 ~~counties~~ 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.