

# Information Technology and Security

## **Purpose**

This policy ensures the security and privacy of data entrusted to Utah's Promise / United Way of Salt Lake (UP/UWSL); the security of information that UP/UWSL collects; and the security of information technology resources that UP/UWSL uses to access data and information. It consists of three sections:

1. Definitions
2. Information technology, acceptable use, and security
3. Equipment policy
4. Policy Review and Updates
5. Contact

## **1. Definitions**

**Information Technology Resource (IT Resource)** – an asset owned, leased, licensed, or maintained by UP/UWSL that processes, stores, or transmits electronic data. IT resources include computers, servers, workstations, mobile devices, networks, computer programs, databases, storage devices, media, printers, photocopiers, facsimile machines, peripheral equipment, gateways, telephones, cellular telephones, personal digital assistants, wireless devices, voicemail, pagers, and other electronic devices including use of the intranet, internet access, web sites, e-mail and related facilities and features. An inventory of UP/ UWSL's physical IT assets worth over \$1,000 is tracked in UP/UWSL's accounting system.

**UP/UWSL Data** – Any form of information used, generated by, or shared with users, including regulated, protected and/or confidential information.

**User** – Any person who is an approved agent of UP/UWSL, including UP/UWSL team members, contractors, Board members, committee members, or other volunteers who are authorized users of UP/UWSL IT resources and/or who have access to or use UP/UWSL data.

## **2. Information Technology, Acceptable Use and Security**

UP/UWSL management is responsible for providing users with guidance and assistance for operating IT resources and accessing or using UP/UWSL data to ensure compliance with regulatory and contractual requirements and the acceptable use requirements set forth in this policy.

### *Policy*

Use of UP/UWSL IT resources, UP/UWSL data, and partner data requires proper authorization. Data stored on UP/UWSL IT resources are the property of UP/UWSL. Use of UP/UWSL IT resources or data may be revoked at any time. UP/UWSL IT resources are to be kept secure. UP/UWSL management expects compliance with all security safeguards, including the use of locked file cabinets and desks, regular password maintenance, never leaving IT resources unsupervised in cars or public places, keeping screens locked when machines are not actively being used, and any other safeguard deemed appropriate.

Sanctions related to violations of UP/UWSL's Acceptable Use Policy are enforced to hold users accountable for their actions when using IT resources, including actions involving poor judgment or illegal activities.

Users acknowledge that their use of IT resources and content or communications received or transmitted through or stored on or within IT resources are subject to review and monitoring and no right to privacy is guaranteed.

UP/UWSL prohibits using IT resources to conduct any of the following. Items outside of these examples that pose legal or security risks to the organization may also be reviewed by the management team as they arise:

#### Legal Matters:

- Send racist, sexist, harassing, or threatening communications, for example using company email to disparage a colleague on the basis of their racial or sexual identity.
- Distribute, communicate, view, access, or display pornography or material that is sexually explicit, offensive, obscene, violent, or otherwise objectionable
- Access, use, or copy computer programs, databases, or copyrighted materials, unless authorized under a license
- Noncompliance with IT resource vendor licensing agreements, including sharing logins as prohibited by such agreements

#### Personal Conflicts:

- Access or disseminate information to facilitate or engage in any violent, criminal, or terrorist act
- Personal gain or the personal gain of others (e.g., political activity, personal business, schoolwork, or commercial enterprise)

#### System Performance:

- Access internet chat rooms, instant messaging, and file sharing outside of business purposes
- Interfere with IT resource performance (e.g. computer processing, internet speed, and storage space)
- Send or forward unsolicited bulk email, chain letters, or spam

#### System Security:

- Jeopardize information and data security, confidentiality, or privacy (e.g., by sharing sensitive information, including information protected by FERPA, HIPAA, or the UP/UWSL Data Privacy Policy)
- Circumvent or disable security, monitoring, filtering, or auditing software or systems
- Other activities prohibited by management

#### UP/UWSL Users are required to:

- Only use IT resources for UP/UWSL business-related work within the scope of employment or contract responsibilities
- Protect identity, passwords, and access numbers
- Comply with privacy and security policies and procedures
- Report inappropriate use of and access to IT resource or theft immediately to their department head or Chief Financial Officer
- Comply with audits of IT resources as requested by management
- Return IT resources upon termination or change in job assignment and notify management when access to specific information or data is no longer required
- Comply with licensing agreements with software vendors
- Users with access to student information protected by FERPA must complete FERPA training annually
- Adhere to the Social Media Policy, Mobile Phone Policy, and Personal and Work Property, Searches, and Inspections outlined in the UP/UWSL Employee Handbook

Users must not infringe on copyrights, trade secrets, or other intellectual property or facilitate, contribute, or induce any infringement.

Software installed on IT resources must be licensed and comply with UP/UWSL policy. Standard software will be loaded onto UP/UWSL hardware by IT staff. Nonstandard software shall not be installed on IT resources without prior approval by IT staff. Non-standard software used for school, personal, family, and/or other civic responsibilities is prohibited. Nonstandard software that is not approved or supported is subject to removal without notice.

Music and videos may be downloaded to IT resources if users comply with applicable copyright law and the downloaded material supports a UP/UWSL business purpose. UP/UWSL reserves the right to remove downloaded music or videos at any time without permission.

Users who violate this policy shall be subject to disciplinary action including termination and/or legal prosecution.

### *Security Standards*

The following security standards and their underlying procedures ensure adequate safeguards are in place to protect and maintain the security and availability of UP/UWSL's information resources.

**Backup and Recovery** – UP/UWSL's IT Support Technician will back up electronic information stored locally in Office 365 at scheduled intervals to secure storage media and facilitate the restoration of all or part of those information resources in the event of loss or corruption of the original data. Users are expected to store local information in cloud-based storage (OneDrive, Sharepoint, etc) to enable periodic backups.

UP/UWSL relies on vendors to back up electronic information in some situations; backup plans for other systems will be created during system onboarding. Backup plans may include using services provided by the vendor.

**Electronic Data Classification** – All electronic data will be classified in one of the following categories:

- Low risk: public information
- Medium risk: internal or select, authenticated external use only
- High risk: protected and business sensitive

Classification of electronic information within these categories will determine the security measures and retention practices used to safeguard UP/UWSL's information resources. For instance, classification of electronic information within each category will determine the following:

- Access rights and requirements
- Where and how the information is stored
- Whether the information is encrypted at rest and during transmission
- Who has authority to release the information for public and internal use

|   | Access  | Storage  | Encryption     | Release   |
|---|---|--|----------------|---|
| <b>Category 1 (Low: Public Information)</b>   |   |  |                |   |
| Public Website  | No requirement  | No requirement   | No requirement | Marketing Dept.   |
| Press Release   | No requirement  | No requirement   | No requirement | Marketing Dept.   |
| Public Reports (Year End, Baseline)   | No requirement  | No requirement   | No requirement | Marketing Dept.   |
| Policies  | No requirement  | No requirement   | No requirement | Marketing Dept.   |
| Created media assets (Blogs, social media posts)  | No requirement  | No requirement   | No requirement | Marketing Dept.   |
| <b>Category 2 (Medium: Internal or Select, Authenticated External Use Only)</b>                 |   |  |                |   |
| General Ledger Database   | Finance Dept.   | Cloud based database hosted by vendor                          | Encrypted      | CFO   |
| Meeting Minutes and Agendas (e.g. Board and Committee Minutes, Meetings with External Partners) | UP/UWSL Staff   | Cloud based storage drive                                      | No requirement | By department and committee leadership                                    |
| Contracts   | UP/UWSL Staff   | Cloud based storage drive                                      | No requirement | By department and committee leadership                                    |
| Bank Account Details  | UP/UWSL Staff   | Cloud based storage drive                                      | No requirement | By department and committee leadership                                    |
| Library of Curated 211 Resource Data  | Named Staff on 211 and Strategy + Data teams and approved other use | Cloud based database hosted by vendor                          | No requirement | 211 Department, subject to Data Sharing Agreements with external partners |
| Aggregate 211 Client Data   | Named Staff on 211 and Strategy + Data teams and approved other use | Cloud based database hosted by vendor                          | No requirement | 211 Department, subject to Data Sharing Agreements with external partners |
| UWSL / UP produced reports citing publicly available aggregate school data                      | Named Staff   | Cloud based storage drive                                      | No requirement | Promise Partnership Department leadership                                 |
| <b>Category 3 (High: Protected and Business Sensitive Information)</b>                          |   |  |                |   |
| Employee Files  | HR and Managers   | Locked physical, cloud-based secure storage drive, HRIS Vendor | Encrypted      | HR  |
| Non Publicly Available Aggregate School Data  | Named Staff   | Cloud-based Storage  | Encrypted      | By statute  |
| Individually Identifiable 211 Client Data   | Named Staff   | Cloud based database hosted by vendor                          | Encrypted      | By statute  |
| Payroll Records   | Named staff   | Hosted by vendor   | Encrypted      | By statute  |
| Donation Processing System  | Named staff   | Hosted by vendor   | Encrypted      | Resource Development  |
| Customer Relationship Management System   | Named staff   | Hosted by vendor   | Encrypted      | By Statute  |
| Student Information   | Staff designated as School Agents                                   | Cloud-based storage database                                   | Encrypted      | FERPA Parental Consent  |
| Server Backups  | IT support technician   | Cloud vendor   | Encrypted      | N/A   |
| Credit Card   | Named staff   | Hosted by vendor   | Encrypted      | N/A   |

Encryption – UP/UWSL will provide secure methods and use of encryption to ensure that while encrypted, data cannot be viewed or otherwise discovered by unauthorized parties in the event of theft, loss or interception.

## *Access Controls*

**Access Rights** – Access to UP/UWSL systems, applications and information is authorized by senior management according to position and work assignment. Access Rights are associated with the individual system ID/User Name. UP/UWSL assigns an admin owner for each system or application who must maintain appropriate access and usage of that system, including adding and removing users according to their access rights. The Strategy and Data team conducts a quarterly audit to ensure admin owners are fulfilling these functions. Individual access rights are reviewed on an as-needed basis, which includes termination of employment and change in function and/or role. UP/UWSL maintains a log of the dates and findings associated with each audit. Access is not granted until a UP/UWSL User has read and signed this policy and completed the appropriate policy review and training.

**Authentication** – Our default position is to use the most advanced, secure authentication method offered by a vendor for their software. Examples include Multi Factor Authentication (MFA), passkeys, and biometric login technology. Single Sign On through Microsoft Entra ID is an acceptable alternative to MFA and should be set up whenever available.

**Shared Access** – Nonpublic access to any UP/UWSL IT resource or any external IT resource involved in doing UP/UWSL business must be granted using individual logins. Logins and passwords may not be shared. Any workbooks, documents, notes (electronic or written) used to share login information are prohibited.

If a system does not allow for multiple accounts to be set up, a shared password vault managed by the IT Technician can be used with approval.

## *Personal Devices*

The use of personal devices for UP/UWSL related work can pose a significant security risk to the organization. Personal devices may not have the same level of security as company-owned devices, and they may be more vulnerable to malware, viruses, and other cyber threats. To minimize these risks, use of personal devices for UP/UWSL work is strongly discouraged except use of phones or smart phones for messaging purposes (Slack, Teams, email) or for authentication. This includes accessing non-messaging systems, documents, or data from personal devices.

If you must use a personal device for work purposes, limit your exposure by only accessing the minimum amount of data necessary to complete your tasks, and by not accessing Level 3 data. Ongoing use of personal devices may prompt the IT team to install software on those devices to protect UP/UWSL data and resources. Storing UP/UWSL data on your personal device(s) is prohibited.

## *Artificial Intelligence, Freeware, and External Applications*

Artificial Intelligence (AI) is evolving rapidly and often embedded directly into IT Resources. Data shared with AI is subject to the same expectations outlined in this policy and the Data Privacy Policy. Providing AI tools with data is to be treated like sharing data with other organizations and individuals. It should not be assumed that data shared with AI tools will be kept confidential. Outputs from AI tools should never be directly applied for work purposes without appropriate review by a team member and/or outside counsel where relevant.

No cost applications that are not on IT's approved application list may share UWSL/UP data in a way that violates UWSL/UP IT and/or Data Privacy Policy. Users are responsible for ensuring the guidelines in the IT and Data Privacy policies are followed. Users that use unapproved IT Resources should understand the Terms and Conditions/

Privacy Policy of that IT Resource. Users are responsible for ensuring that unapproved IT Resources have appropriate protections to protect UWSL/UP data. When using freeware or free or paid versions of applications (e.g. Otter, Miro, template creation tools, etc) users should not assume data provided to those tools is kept private.

### *UP/UWSL Network Infrastructure Protections*

A physical firewall device must be configured to block all incoming traffic by default, except for traffic that is explicitly allowed by the organization's security policies. Additionally, the firewall must be configured to log all traffic that passes through it, so that any suspicious activity can be detected and investigated.

Wi-Fi access points must be secured with strong passwords and encryption protocols to prevent unauthorized access. Additionally, wireless networks must be segmented from the rest of the network to minimize the risk of a breach. All Wi-Fi access points must be configured to use WPA2 encryption or higher.

Switches must be configured to limit access to the network and prevent unauthorized changes to the network configuration. This includes disabling unused ports, enabling port security, and configuring VLANs to segment the network. Physical access to switches must be limited to approved personnel, and switches are to be monitored for unusual activity or signs of tampering.

All UP/UWSL owned devices have anti-virus software installed and enabled. Additionally, all devices have firewalls enabled and properly configured.

### *Password Management*

- User passwords should contain characters from three of the following categories:
  - Uppercase
  - Lowercase
  - Base 10 digits (0 through 9)
  - Non-alphanumeric characters (e.g., ~!@#\$%^&\*()+-={}:;<>[]\;',./)
- Password must not contain the user's first or last name
- Password must be unique and cannot have been used by the user previously
- Password length must be at least 16 characters in length\*

\*Character length may be shortened if software solution does not permit 16 characters.

Passwords should not be written down. The use of approved password manager tools is allowed.

### *Security Incident Response*

UP/UWSL Users are responsible for reporting known or suspected information or information technology security incidents. All security incidents at UP/UWSL must be promptly reported to UP/UWSL's Chief of Staff, who will review and assess the events.

A security incident is any real or suspected event that may adversely affect UP/UWSL security, UP/UWSL Data and/or Partner Data, and/or the systems that process, store, or transmit that information. Examples of incidents may include:

- Unauthorized access to, storage of, or sharing of data
- Systems infected with malware such as a worm, virus, Trojan Horse or botnet

- Reconnaissance activities such as unauthorized scans of the network and/or systems
- Denial of service attacks
- Phishing attacks
- Website and/or Social Media defacement
- Use of unauthorized tools to detect or exploit vulnerable or un-patched systems

An incident response will be handled appropriately based on the type and severity of the incident in accordance with the Incident Response Summary Table below. Handling of security incidents involving confidential data (including personally identifiable information) will be overseen by the Incident Management Team (as defined below).

UP/UWSL’s Chief of Staff will be the **Incident Response Manager** and is responsible for managing the response to a security incident as defined in the incident response summary table below.

The **Incident Management Team** has the authority to make decisions related to the incident and to notify appropriate parties. The team consists of six core members and others as appointed by the Chief of Staff.

The Incident Management Team members are:

- Chief of Staff (incident response manager)
- IT Support Technician
- Senior Director, Strategy and Data
- Senior Director, People Operations
- The Supervisor of any individual responsible for any alleged incident
- UP and/or UWSL Board Chair & Vice Chair (when applicable)

Other members may include the Finance Chair, UP/UWSL President & CEO, the Chief Financial Officer and/or Chief Development Officer (e.g., if the incident involves donor data), other UP/UWSL team members who administer specific software systems, and/or legal representation.

The following table summarizes the handling of UP/UWSL security incidents based on severity, including response time, the responsible incident managers, and notification and reporting requirements. Reporting requirements should be understood to include tracking for high and medium incidents including their cause, nature, source, and resolution and tracking of the frequency of low incidents. Reporting and discussions of these incidents will be made as needed to the Incident Response Team and Finance Committee.

| Incident Response Summary Table |   |   |   |   |
|---------------------------------|---|---|---|---|
| Incident Severity               | Minimum Security Characteristics  | Response Time   | Incident Manager                                | Others Incident Manager Will Notify   |
| <b>HIGH</b>                     | 1. Significant adverse impact on a large number of systems and/or people<br>2. Potential large financial risk or legal liability to UP/UWSL<br>3. Threatens confidential data<br>4. Adversely impacts a critical system or service<br>5. Significant and immediate threat to human safety<br>6. High probability of propagating to a large number of other systems onsite or off site, causing significant disruption | Immediate   | UP/UWSL Chief of Staff                          | UP/UWSL CEO, CFO,<br>Other Senior Management,<br>Finance Committee Chair, UP/UWSL IT Support Technician<br><br>Incident Response Team |
| <b>Medium</b>                   | 1. Adversely impacts a moderate number of systems and/or people, i.e. a single department, or users in a narrow role<br>2. Adversely impacts a non-critical enterprise system or service<br>3. Adversely impacts a departmental scale system or service<br>4. Disrupts a building or departmental network<br>5. Moderate risk of propagating and causing further disruption   | 8 hours or less (by end of business day reported)           | UP/UWSL Chief of Staff or IT Support Technician | Chief of Staff, CFO, UP/UWSL IT Support Technician Director, Strategy and Data, Department Manager                                    |
| <b>Low</b>                      | 1. Adversely impacts a very small number of non-critical individual systems, services, or people, for example with no connection to PII, payment processing, or ability to post or represent the organization<br>2. Disrupts a very small number of network devices or segments<br>3. Little risk of propagation and further disruption   | By end of business day following incident report, or sooner | IT Support Technician                           | Chief of Staff, Senior Director, Strategy and Data Department Manager   |
| <b>N/A</b>                      | "Not Applicable" – used for suspicious activities which upon investigation are determined not to be an IT security incident.  |   |   |   |

The Chief of Staff will provide the CEO and CFO a quarterly summary of breaches in the "Low" risk category.

### 3. Equipment Policy

This section applies to employees that are issued a desktop or laptop computer owned by UP/UWSL. Our work requires that computing resources are current and operating at optimal performance. To meet these requirements, a minimum standard for computing resources has been outlined to increase the supportability of UP/UWSL's installed base of equipment.

#### *Computer Peripherals*

UWSL will provide full-time team members that have dedicated, in-office workspaces with one set of standard peripherals for use in their in-office workspace. The set of peripherals include:

- 1 External monitor
- 1 Docking station
- 1 Mouse



- 1 Keyboard
- 1 Headset (if requested)

Dual external displays and/or larger external displays may be provided to team members with technology-centric roles. Dual external displays are a pair and are to be kept together in the same work location. A 3rd external display may be issued in rare circumstances.

Peripherals desired for a secondary work location are the team member's responsibility. Team members who do not have a dedicated workspace in UP/UWSL offices will have access to peripherals when working in the office. For these team members, taking peripherals from shared workspaces in the office to other locations is not allowed.

### *Replacement*

UP/UWSL will replace desktop, laptop, and tablet computers every four years, or as funding allows. One year prior to the replacement date of each computer, the IT support technician will perform a diagnostic review of the functionality of the computer to determine if the replacement date should be adjusted.

If a staff member accepts a new role at UP/UWSL, that staff member may be issued a computer associated with the new job function and/or department.

### *Hardware Standards*

To maintain a reliable and efficient computing environment for all users of the UP/UWSL network, UP/UWSL has adopted certain standards. The purpose of these standards is to:

- Optimize the support levels that IT provides
- Manage the cost of purchasing, replacing and support of technology at UP/UWSL
- Improve service using automatic deployment of software
- Ensure that there is network compatibility for security and upgrades

UP/UWSL's network runs on Microsoft Entra ID technologies using Microsoft services. All staff workstations will operate using Windows Professional. The default workstation will be a Windows PC, and UP/UWSL's technical infrastructure is designed to support Windows PCs. However, users who have experience using Macs with Office 365 and prefer a Mac may request a Mac as their workstation at the time they are hired or when their machine is up for replacement. IT support for Mac users will be lighter, may be slower than for Windows PC users, and may be outsourced to an external consultant.

Due to the standards, only certain models of computers from specific manufacturers are supported. The following computer models are fully supported by IT:

#### *Desktops*

Dell OptiPlex Models 3000 and above.

Any other Dell desktop computer is not supported– including Inspiron, Vostro and XPS.

#### *Laptops*

All Dell Latitude E 7000 series laptops.

Any other dell laptop computer is not supported– including Inspiron, XPS, Adamo, or gaming laptops.

#### *Tablets*

Microsoft Surface Pro, Apple iPad Air, iPad Mini 3

Apple Desktops  
Apple iMac, Mac Mini

Apple Laptops  
Apple MacBook Pro, MacBook Air

Keyboard and Mice  
Bluetooth wireless mouse and keyboard (will be phased in as replacements are needed)

Monitors  
23" widescreen (will be phased in as replacements are needed)

UP/UWSL has a base configuration for computer workstations and peripherals that protects UP/UWSL resources by ensuring standard models are available as team members turn over. Variations on that base configuration for a specific business purpose can be approved by a Department Head. Other types of exceptions must be approved by the CEO and adhere to the security standards outlined in this policy, in coordination with the IT team. If team members are seeking an exception because hardware that has been issued does not meet their needs, they should submit an IT request and have UP/UWSL's IT team assess the team member's current hardware.

#### *Disposal of Retired Equipment*

To protect sensitive data stored on UP/UWSL computing resources, retired computers, tablets, mobile phones, and all devices that store data will not be made available for sale or donation. All old equipment will have its hard drive removed and destroyed onsite by the IT Support Technician and then sent to a Utah State licensed e-recycling facility to be disassembled or destroyed by the IT Support Technician if possible.

In rare cases, UP/UWSL computing resources may be donated. Under exigent circumstances (e.g., when there are students, parents, or other community members who would benefit from retired equipment), members of UP/UWSL leadership team may authorize the donation of equipment. Before donating equipment, UP/UWSL will eliminate the risk that any sensitive information previously stored on the machine will become accessible by: (1) removing and destroying the existing hard drive(s) and (2) replacing the removed hard drive(s) with factory-sealed, clean hard drives. UP/UWSL will transfer full rights of ownership to the intended owner and will require the recipient to sign a release of liability for donated equipment.

#### *IT Resource Purchases*

All purchases of IT resources must be coordinated by the Strategy and Data team. By coordinating all IT purchases, we can avoid duplication of resources and ensure that all equipment is compatible with our existing systems. Additionally, this policy helps us monitor costs and ensures that we are making the most efficient use of our resources.

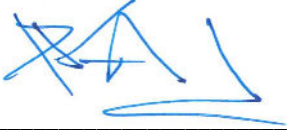
## 4. Policy Review and Updates

This policy is subject to review every three years by the UP / UWSL Finance Committee and Boards of Directors, and to periodic review by our IT team. Internal reviews are conducted at least annually, or more frequently if significant changes to data practices, regulations, or technology warrant immediate attention. Reviews may include incorporating staff or stakeholder feedback, the results of internal audits, and emerging changes in privacy laws and regulations. Certain changes may warrant updates to the UP/UWSL website and/or email communication to constituents or staff, to be determined by UP/UWSL leadership.

## 5. Contact

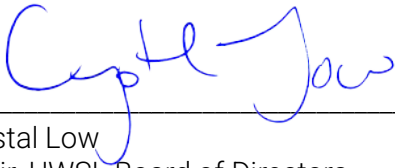
For inquiries, concerns, or requests related to this policy or IT security at UP/UWSL more generally, please contact [data@utahspromise.org](mailto:data@utahspromise.org).

Adopted this 18th day of January 2024



---

Kirk Aubry  
Chair, UP Board of Directors



---

Crystal Low  
Chair, UWSL Board of Directors

### Signatures

I have read and understand Utah's Promise / United Way of Salt Lake's Information Technology and Data Privacy Policy. I will neither share nor discuss the Data – verbally or in writing – with any other party (unless that party has signed a data confidentiality agreement substantially similar to this one). I agree that, in explaining our collective impact work, I will use information that is widely available to the general public. Further, I will immediately notify UP/UWSL if I become aware of any actual or potential unauthorized data disclosure and understand that in no case may the Data be shared with the media, funders, and/or the general public, without written permission of the agency that provided the Data. Sharing – whether verbally or in writing – any or all of this Data could result in a termination of relationship with UP/UWSL and/or termination of other supports provided by UP/UWSL and/or legal action. Finally, I understand that even if UP/UWSL does not distribute this Form at a convening where data is discussed, UP/UWSL does not waive the above requirements for confidentiality.

Name (print): \_\_\_\_\_

Date: \_\_\_\_\_

Organization: \_\_\_\_\_

Signature: \_\_\_\_\_

*NOTE: UP/UWSL will retain these data request forms in secure locations*