ADVANCING EDUCATION
INCOME AND HEALTH

LIVE UNITED
United Way

United Way of Salt Lake
*serving Davis, Salt Lake, Summit, and Tooele Counties*

policy

# Information Security Policy

***September 11, 2018***

**Purpose**

This policy ensures the security of data entrusted to United Way of Salt Lake (UWSL); the security of information that UWSL collects; and the security of information technology resources that UWSL uses to access data and information. It consists of seven sections:

1. Definitions
2. Partner Data acceptable use and security
3. Information technology, acceptable use, and security
4. Donor information privacy
5. Document retention and destruction
6. Computer replacement
7. Acknowledgement of receipt

## 1. Definitions

**Information Technology Resource (IT Resource)** – an asset whether owned, leased, licensed or maintained by UWSL that, processes, stores, or transmits electronic data. IT resources include but are not limited to 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 UWSL's IT Resources is maintained by UWSL's Finance Department.

**Personally Identifiable Information (PII) –** information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personally identifiable information which is linked or linkable to a specific individual. Personally identifiable information may include an individual's name (first name and last name, or first initial and last name) in combination with one or more of the following: date of birth, home address, employee social security number, driver's license number or state identification card number, mother's maiden name, electronic identification numbers, electronic signature or financial account number, or credit or debit card number, alone or in combination with any required security code, access code or password that would permit access to a consumer's financial account.

**UWSL Data** – any form of information utilized, generated by, or shared with UWSL Users including regulated, protected and/or confidential information.

**Partner Data** – a specific type of UWSL Data that is not generated by UWSL but which is entrusted to UWSL to support UWSL in playing backbone coordinating functions in service of one or more population-level outcomes. This includes regulated, protected and/or confidential information.

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

## 2. Partner Data Acceptable Use & Confidentiality

This section describes protections related to Partner Data.

***Policy***

UWSL recognizes that our most complex social problems – including the achievement gap, poverty, and healthcare access – cannot be solved by any one organization on its own. It is only by working together and holding accountability for specific outcomes for our entire community that the cycle of poverty will end. This accountability requires the sharing of appropriate aggregated data (and - for certain staff - of individual level data, in ways that comply with state and federal law).

The Partner Data that is shared with UWSL is intended for continuous improvement around shared community goals. Intended uses for Partner Data include: recruiting students into initiatives; providing targeted support(s) to students; tracking progress and outcomes; and developing, aligning, and implementing interventions (including policy-level interventions) aimed at moving population-level indicators.

Partner Data is a reflection on the entire community, which shares accountability for current reality and for future results. It is not, and cannot be used, as evidence of the success or failure of one particular program, organization, sector, or population. Partner Data cannot be used in communications with media, funders, or the general public without the written permission of the data provider(s) and without complete context and clear acknowledgement of the broadly shared accountability for results.

The guiding principle in sharing Partner Data is the protection of clients' information. By informing students, families, and data contributors about how their information will be used, and by protecting it when it is provided, we will build more trust in our communities. This agreement is part of a practice developed to maintain this trust. An overview of our data security practices is available at uw.org/data.

Further, Partner Data may not be shared or discussed with any other party, unless such party is an approved partner with legitimate interest in the data and has signed a data confidentiality agreement.

Information compiled and presented by an institution about its own programs, initiatives, etc. may be used according to the policies and practices of that institution without restriction. UWSL is not responsible for data use and presentation by a specific institution about its own programs.

Sharing – verbally or in writing – any of this data could result in a termination of relationship with UWSL and/or termination of other supports provided by UWSL and/or legal action. UWSL maintains a list of vetted and approved data points that are available for staff, Board members, and partners and are encouraged to use as a source to describe needs and successes.

## 3. Information Technology, Acceptable Use and Security

This section defines the proper use of information technology (IT) resources owned by UWSL and UWSL Data residing on personal or other parties' IT resources. UWSL management is responsible for providing UWSL Users guidance and assistance for operating IT resources and accessing or using UWSL Data to ensure compliance with regulatory and contractual requirements and the acceptable use requirements set forth in this policy. It applies to all users operating or accessing IT resources and data managed or owned by UWSL.

***Policy***

Use of UWSL IT resources, UWSL Data, and Partner Data requires proper authorization. Data stored on UWSL IT resources are the property of UWSL. Use of UWSL IT resources or data may be revoked at any time. UWSL IT resources should be kept secure. UWSL management expects full compliance with all security safeguards including the use of locked file cabinets and desks, regular password maintenance, rigor around never leaving IT resources unsupervised in cars or public places, and any other safeguard deemed appropriate by management.

Inappropriate use of UWSL IT resources and data is prohibited. Sanctions related to violations of UWSL's Acceptable Use Policy are communicated to users and enforced to hold users accountable for their actions when using IT resources, UWSL Data and Partner Data, including actions involving poor judgment or illegal activities.

IT resources are monitored and UWSL Users consent to such monitoring either with or without advance or subsequent notice. UWSL 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 granted.

UWSL prohibits using IT resources to conduct any of the following:

Legal Matters:

- To send racist, sexist, harassing, or threatening communications
- Distribute, communicate, 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

Personal Conflicts:

- Access or disseminate information to facilitate or engage in any violent, criminal, or terrorist act

- Use IT resources for personal gain or the personal gain of others (e.g., political activity, personal business or commercial enterprise)

System Performance:

- Internet chat rooms, instant messaging (other than those approved for business purposes), and file sharing
- 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
    - Sharing sensitive information, including information protected by FERPA, HIPAA, or UWSL's Data Confidentiality Policy.
- Circumvent or disable security, monitoring, filtering, or auditing software or systems
- Other activities prohibited by management

UWSL Users are required to:

- Use IT resources for 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 the department director or Chief Financial Officer
- Comply with audits of their 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 all other aspects of this policy
- UWSL Users with access to student information protected by FERPA must complete FERPA training biannually
- Adhere to Social Media Policy (section 5.4.2), Mobile Phone Policy (section 5.5), and Personal And Work Property, Searches, and Inspections (section 5.9) outlined in the UWSL Employee Handbook

UWSL 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 UWSL policy. Standard software will be loaded onto UWSL Hardware by appropriate IT staff. Nonstandard software must not be installed on IT resources without prior approval by IT staff. With no exception, non-standard software used for school, personal, family, and/or other civic responsibilities is prohibited. Nonstandard software that is not approved and supported and is subject to removal.

Music and videos may be downloaded to IT resources as long as UWSL Users comply with applicable copyright law and the downloaded material supports a UWSL business purpose.

UWSL reserves the right to remove downloaded music or videos at any time without permission.

Violation of this policy shall be subject to disciplinary action including termination and/or legal prosecution.

***Security Standards***

The following security standards and their underlying procedures provide guidance and instruction to ensure adequate safeguards are in place to protect and maintain the security and availability of UWSL's information resources:

**Backup and Recovery –** UWSL's IT contractor will back up electronic information resources at scheduled intervals to suitably 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.

***Information Security***

**Electronic Data Classification –** UWSL's senior management team will classify all electronic data in their areas of responsibility within the following three categories:

- Low risk: public information
- Medium risk: internal use only
- High risk: protected and business sensitive

| | **Access** | **Storage** | **Information** | **Release** |
|---|---|---|---|---|
| **Category 1 (Low, Public Information)** | | | | |
| 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. |
| Media | No requirement | No requirement | No requirement | Marketing Dept. |
| **Category 2 (Medium, Internal Use Only)** | | | | |
| Bookkeeping Database | Finance Dept. | Cloud based database hosted by vendor | Encrypted | CFO |
| Meeting Minutes | UWSL Staff | Local server, cloud based storage drive | No requirement | By department and committee |

| | | | | |
|---|---|---|---|---|
| Contracts | UWSL Staff | Document server, cloud based storage drive | No requirement | By department and committee |
| Publicly Available Aggregate School Data | Named Staff | Local server and cloud based storage drive | No requirement | CI Department |

| **Category 3 (High Protected and Business Sensitive Information)** | | | | |
|---|---|---|---|---|
| Employee Files | HR and Managers | Locked physical | No Transmission | HR |
| Non Publicly Available Aggregate School Data | Named Staff | Local servers,, cloud-based student database, SFTP Server | SFTP | By statute |
| Payroll Records | Named staff | Hosted by vendor | Encrypted | By statute |
| Donation Processing System | Named staff | Local server | Encrypted | Finance Department |
| Customer Relationship Management System | Named staff | Hosted by vendor | Encrypted | By Statue |
| Student Information | School Agents | Local servers, cloud-based student database, SFTP Server | SFTP | FERPA Parental Consent |
| Server Backups | IT Consultant | Cloud vendor | Encrypted | N/A |
| Employee Health Files | HR and Employee Record | Locked physical | Check w/ Operations Director | HR and statute |

Classification of electronic information within these categories will determine the security measures and retention practices used to safeguard 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

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

**Access Rights** – Access to UWSL systems, applications and information is dependent on senior management's authorization and the individual's position in the organization and work assignment. Access Rights are associated with the individual system ID which enables the assignment of appropriate Access Rights to applications and information resources necessary to do their work. An audit is conducted quarterly to monitor all Access Rights. Individual Access Rights are reviewed on an as-needed basis, which includes but not limited to; termination of employment and change in function and/or role. Access is not granted until a UWSL User has read and signed this policy and completed the appropriate policy review and training. UWSL maintains a log of the dates and findings associated with each review. This log includes an accounting of what each end-user has attempted to access, relative to their authorized rights.

**Password Management** –

- User passwords must contain characters from three of the following categories:
    - Uppercase
    - Lowercase
    - Base 10 digits (0 through 9)
    - Non-alphanumeric characters (~!@#$%^&*()+-={}:<>[]\;',./)
- Password must not contain the user's first or last name
- Password must be changed annually
- 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

**Security Incident Response –** UWSL Users are responsible for reporting known or suspected information or information technology security incidents. All security incidents at UWSL must be promptly reported to UWSL's Chief Operating Officer, who will review and assess the events.

A security incident is any real or suspected event that may adversely affect the security of UWSL, 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 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 will be overseen by the Incident Management Team.

UWSL's Chief Operating Officer (COO) 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** oversees the handling of security incidents involving confidential data (e.g., personal identity information) and any breach to these policies. This team has authority to make decisions related to the incident and to notify appropriate parties. The Incident Management Team consists of six core members and others as appointed by the COO.

The Incident Management Team members are:

- Chief Operating Officer (incident response manager)
- IT Contractor
- Senior Director, Data Operations
- Vice President, Human Resources & Operations
- The Supervisor of any individual responsible for any alleged incident
- Board Chair & Vice Chair (when applicable)

Other members may include the Data & IT Security Committee Chair, UWSL President & CEO, other UWSL employees who administer specific software systems, and/or legal representation.

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

| **Incident Response Summary Table** | | | | |
|---|---|---|---|---|
| **Incident Severity** | **Minimum Security Characteristics** | **Response Time** | **Incident Manager** | **Others Incident Manager Will Notify** |
| **HIGH** | 1. Significant adverse impact on a large number of systems and/or people<br>2. Potential large financial risk or legal liability to UWSL<br>Threatens confidential data<br>3. Adversely impacts a critical system or service<br>4. Significant and immediate threat to human safety | Immediate | UWSL COO | UWSL CEO<br>Other Senior Management<br>IT Security Committee Chair<br>UWSL IT Contractor<br>Incident Response Team |

| | | | | |
|---|---|---|---|---|
| | 5. High probability of propagating to a large number of other systems onsite or off site, causing significant disruption | | | |
| **Medium** | 1. Adversely impacts a moderate number of systems and/or people<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 | UWSL COO or IT Contractor | COO<br>UWSL IT Contractor Director, Data Operations Department Manager |
| **Low** | 1. Adversely impacts a very small number of non-critical individual systems, services, or people<br>2. Disrupts a very small number of network devices or segments<br>3. Little risk of propagation and further disruption | Next business day | IT Contractor | COO<br>Senior Director, Data Operations Department Manager |
| **N/A** | "Not Applicable" – used for suspicious activities which upon investigation are determined not to be an IT security incident. | | | |

## 4. Donor Information Privacy

The following section governs the collection and retention of contributor information.

***Policy***

Contributors are requested to provide certain personal information to UWSL, such as home address, phone number, e-mail, and other contact information. The primary purpose for obtaining this information is to allow UWSL to comply with donors' restrictions and designations, to provide donors with charitable gifting tax information, for donor recognition and communication, and to facilitate fundraising and other engagement opportunities. The information is retained in the financial records of UWSL for financial recording and internal financial accounting control purposes.

To protect the confidentiality of personal information, UWSL uses appropriate technical and internal control measures to limit access to and control the retention of the information to ensure its use and access is limited to the above noted purposes.

- Personal information obtained by UWSL will not be communicated outside of UWSL unless required by law, to facilitate fundraising, or as authorized by the donor. UWSL will include a provision of confidentiality in all contracts and agreements with all third-parties that will have access to donor information.

- As noted in the information security section of this policy, access to information housed in UWSL systems is dependent on senior management's authorization and the individual's position in the organization and work assignment. All access rights are reviewed for all UWSL Users quarterly, and for individual UWSL Users upon termination of employment or upon internal job transfer.
- UWSL does not sell or rent donor information of any kind to outside parties.
- Donors may review their personal information and specify corrections to this information, oppose the retention of the information, or request its elimination from
- UWSL records. Changes can be emailed to UWSL's Chief Marketing & Engagement Officer.UWSL retains personal information only as long as necessary for the purposes stated and to comply with federal and state record retention requirements.

## 5. Document Retention and Destruction

This section identifies the record retention responsibilities of employees for maintaining and documenting the storage and destruction of the organization's documents and records.

Employees are required to abide by the following rules:

- Paper or electronic documents indicated under the terms of the retention table in the following section will be the responsibility of and will be maintained by appropriate UWSL staff based on role and responsibility.
- Unless needed for ongoing business purposes and reference all other documents will be destroyed after three years;
- Unless needed for ongoing business purposes and reference all other email and electronic documents will be deleted from all individual computers, mobile devices, databases, networks, and back-up storage after three years;
- No paper or electronic documents will be destroyed or deleted if pertinent to any ongoing or anticipated government investigation, proceeding, or private litigation (check with legal counsel or the human resources department for any current or foreseen litigation if employees have not been notified); and
- No paper or electronic documents will be destroyed or deleted as required to comply with applicable Federal, State and Local laws or with government auditing standards (Single Audit Act)
- Emails of a personal non-business nature should be deleted immediately.

***Record Retention***

The following table indicates the minimum requirements for record retention. In addition, federal awards and other government grants may provide for a longer period than is required by other statutory requirements.

| File Category | Item | Retention Period |
|---|---|---|

| | | |
|---|---|---|
| **Accounting and Finance** | Accounts Payable ledgers and schedules | 7 years |
| | Accounts/Pledges Receivable ledgers and schedules | 7 years |
| | Annual Audit Reports and Financial Statements | Permanent |
| | Annual Audit Records, including work papers and other documents that relate to the audit | 7 years after completion of audit |
| | Bank Statements and Canceled Checks | 7 years |
| | Expense Records | 7 years |
| | General Ledgers | Permanent |
| | Electronic Payment Records | 7 years |
| | Notes Receivable ledgers and schedules | 7 years |
| | Investment Records | 7 years after sale of investment |
| | Insurance policies and contracts | Permanent |
| **Corporate Records** | Annual Charitable Permit registrations - State of Utah | 7 years after expiration |
| | Articles of Incorporation | Permanent |
| | By-laws | Permanent |
| | Board Meeting and Board Committee Minutes | Permanent |
| | Board Policies/Resolutions | Permanent |
| | IRS Application for Tax-exempt Status (Form 1023) | Permanent |
| | IRS Determination Letter | Permanent |
| | State Sales Tax Exemption Letter | Permanent |
| | Contracts (after expiration) | 7 years |
| | Licenses and Permits | 7 years after expiration |
| **Employee Documents** | Benefit Plans | Permanent |
| | Employee Files | Termination + 7 years |
| | Employment applications, resumes and other forms of job inquiries, ads or notices<br>for job opportunities | 3 years |
| | Forms I-9 | 3 years after hiring, or 1 year after separation |
| | Employment Taxes | 7 years |
| | Payroll Registers and payroll tax returns | 7 years |
| | Time Cards/Sheets | 7 years |
| | Unclaimed Wage Records | 7 years |
| | Retirement and Pension Records | Permanent |

| | | |
|---|---|---|
| **Property Records** | Lease Agreements | Permanent |
| | Depreciation Schedules/Asset Inventories | 7 years after asset disposed |
| **Tax Records** | Tax-Exemption Documents and Related Correspondence | Permanent |
| | IRS 990 and 990T tax returns | Permanent |
| | Tax Bills, Receipts, Statements | 7 years |
| | Sales/Use Tax Records | 7 years |
| **Grants awarded to UWSL** | Original grant proposal | 7 years after completion of grant period or longer depending on contractual agreements, applicable laws and/or program needs |
| | Grant agreement and subsequent modifications, if applicable | 7 years after completion of grant period or longer depending on contractual agreements, applicable laws and/or program needs |
| | Final grantee reports, both financial and narrative | 7 years after completion of grant period or longer depending on contractual agreements, applicable laws and/or program needs |
| | All evidence of returned grant funds | 7 years after completion of grant period or longer depending on contractual agreements, applicable laws and/or program needs |
| | All pertinent formal correspondence including opinion letters of counsel | 7 years after completion of grant period or longer depending on contractual agreements, applicable laws and/or program needs |
| | Report assessment forms | 7 years after completion of grant period or longer depending on contractual agreements, applicable laws and/or program needs |

| | | |
|---|---|---|
| | Documentation relating to grantee evidence of invoices and matching or challenge grants that would support grantee compliance with the grant agreement | 7 years after completion of grant period or longer depending on contractual agreements, applicable laws and/or program needs |
| | Documentation of grantee work product and outcomes | 7 years after completion of grant period or longer depending on contractual agreements, applicable laws and/or program needs |
| **Contribution Records** | Pledge forms, pledge letters and all correspondence related to donor restrictions | 7 years after completion of grant period or longer depending on contractual agreements, applicable laws and/or program needs |
| | Planned giving documents including wills, trusts, annuities, bequests, endowments and correspondence and restrictions pertaining thereto. | Permanent |
| **Program services records including grants awarded by UWSL** | Grantee applications, grantee contracts and addenda, grantee correspondence, grantee outcomes and performance reports, program statistical data and outcomes, data waivers, and research performed and/or published | 7 years after completion of grant period or longer depending on contractual agreements, applicable laws and/or program needs |

## 6. Computer Replacement Policy

This section applies to employees that are issued a desktop or laptop computer owned by UWSL. Business necessity 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 UWSL's installed base of equipment.

***Replacement***

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 contractor will perform a diagnostic review of the functionality of the computer to determine if the replacement date should be adjusted.

In the event that an existing staff member accepts a new position within a different department at UWSL, that staff member would not retain their same computer in their new job functions but would rather be issued a computer associated with the new job function and department.

In the event that an existing staff member accepts a new position within the same department to which they already are a member, at the discretion of the department head, they would retain their same computer in their new job functions.

### *Hardware Standards*

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

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

UWSL's network runs on Microsoft Active Directory technologies using Windows Servers. All staff workstations will be PCs with the exception of select team members with specific engagement and design responsibilities. Due to the standards, only certain models of computers from specific manufacturers are supported. Many computer models are not designed for networked business needs and are more suitable for home or gaming use. 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

**Marketing Desktops**
Apple iMac

**Marketing Laptops**
Apple MacBook Pro

Any exceptions to these standards must be approved in writing in advance by the CEO.

### Disposal of Retired Equipment

To protect any and all sensitive data that is stored on 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 IT Contractor and then sent to a Utah State licensed e-recycling facility to be disassembled.

We recycle other devices at:

Salt Lake Valley Solid Waste Facility
1400 South 6030 West

Adopted this 14th Day of June, 2018.

________________________________________
Scott Ulbrich
Chair, Board of Directors

## 7. Receipt and Acknowledgement

By signing below, I affirm that I have read UWSL’s information security policy and agree to abide with the provisions within.

Name *(print)*:

Date:

Signature: