# Vendor Service Tech
# VIU Account Request Form

Open with **Adobe Reader** to fill in the fields below, then save the completed form with a new file name.
Return the completed form(s) to your VIU contact person.
VIU contact person will submit the form as an email attachment to **ITHelp@viu.ca**.
An IT ticket will be created for your request and your VIU contact person will be in touch once the account has been created.

| | | | |
|---|---|---|---|
| Vendor Company Name | | | |
| Vendor Manager Name | | | |
| VIU Contact Names | main: | secondary: | |
| 1st Technician | Name | Email | Phone |
| 2nd Technician | Name | Email | Phone |

If there will be more than 2 technicians who may visit VIU for warranty or other service work, please complete page 3 for the additional technicians. Make sure you include with full names, email addresses, and phone numbers.

The Vendor Manager will be responsible for ensuring **each technician who requires elevated access,** has **read and signed** a copy of the **VIU ELUP terms** (page 2 of this document). You can save multiple copies of the form as needed.

Even if there are no admin rights granted , pages 4- 9 outline the VIU **Use of Information Technology** Policy 45.01(note: Policy 45.01 is under review and a new version will be sent when completed). Vendor Managers must ensure that their technicians read the policy and comply to the terms that relate to the work being undertaken on VIU computers and servers.

The Vendor Manager must also contact their VIU contact person to request that the VIU computer account be removed if any technicians leave the company.

**Scope of Work being done** - let us know what the techs will need when they come to VIU so we can determine the level of access required for the account. Please fill out all boxes that apply for ALL techs included on this form:

If access requirements vary with different Technicians, leave this part blank and include the technicians in the list on page 3, and clarify the additional access needs for each individual Technician.

Will the work being performed be "as needed" **warranty service,** or part of an **existing service agreement** for system upgrades or periodic maintenance? ☐ warranty ☐ Service Agreement

Will the account(s) require **Elevated Local User Privileges**(ELUP)? ☐ Yes ☐ No

Will a **VIU IT Tech** need to be on hand to assist with the work being performed? ☐ Yes ☐ No
Please provide the VIU tech name(s) if you know it, or let us know which team you need assistance from:

Will all work be done **On-Site** at VIU or is there a requirement for **remote access**? ☐ on-site ☐ remote

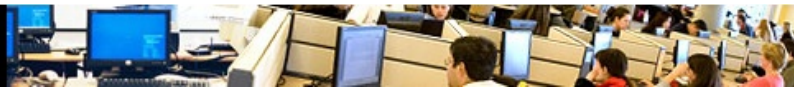
If on-site, is there a **specific location for service**, provide building and room numbers if possible. If not working in a specific location consistently, enter "various".

Will the service needed require **Internet** and/or **VIU network** Access ☐ internet ☐ VIU network

For site visit and remote access, provide the **name(s) for the computer, server, website or application** that the tech will need access to. If not working on specific equipment consistently, enter "various"

Will the technicians require access to the **VIU VPN** to perform the service Provide ☐ Yes ☐ No

any other requirements your tech(s) will need from VIU staff for this account:



# Elevated Local User Privileges (ELUP) – VENDOR Service Techs

These ELUP terms are for Service Technicians from Vendors who will have administrative access to VIU computer and systems. If you do NOT need elevated user privileges, you do not need this step.

A VIU computer service account with Elevated Local User Privileges (ELUP), will only be granted to qualified vendor technicians who understand the risks associated with this type of account and agree to the terms below.

If your company will have multiple Technicians providing service to VIU, a Technician manager should ensure that **each technician** receives and signs a copy of this agreement. The Technician manager will supply a copy of all signed agreements to their VIU contact person, who will pass the forms along to the VIU IT department.

Please read the following "Use of Elevate Local User Privileges (ELUP) Agreement" and sign the form where indicated as your agreement to the terms below:

### *Elevated Local User Privilege Agreement*

*When granted Elevated Local User Privileges on a VIU computer you must:*

1. *Comply with all related VIU Policies that relate to the work being undertaken, including VIU's Policy 45.01 Use of Information Technology* (refer to pages 4-9)
2. *Never share the VIU account details with any other person.*
   a. *If more than one technician is sharing one account, the Technician Manager will provide the account details to each technician as needed.*
3. *Contact ithelp@viu.ca and request to work with an IT Tech if you will need to un-install, replace, or reconfigure any VIU IT loaded applications or system policies on the computer.*
4. *Ensure any software loaded onto the computer has appropriate license terms so it can be legally used in an enterprise environment.*
5. *Be vigilant when using the computer and immediately report any strange behaviour to ithelp@viu.ca as quickly as possible. Please provide the computer name, and mention your company name, your name and provide your VIU account name.*
6. *Understand that if a computer becomes unstable or unusable IT may re-image the computer back to a default standard state. This may cause you and any other user that has logged into this computer to lose all data saved locally and any customizations.*
7. *Agree to not access other user profiles and local files that may be present on the computer.*
8. *Elevated Local User Privileges are granted on an annual basis, but the account will only be activated for scheduled work dates and times.* *(All visits must be scheduled with your VIU contact person)*
   a. *Your Company will be contacted by IT to reconfirm your ELUP agreement within two weeks of the anniversary date on which they were granted.*

Tech Full Name

Company Name

Tech Signature

Date signed

# List of Additional Techs for va_accounts:

In addition to the 2 technicians listed on page 1, please supply the following information for any extra accounts needed.

If the access requirements are the same for ALL technicians, please make sure page 1 has all the details and Check the Use Page 1 Access requirements box, and leave the Special Access Requirements box blank.

If any of the additional technicians need special access, please add that information in the Special Access Requirements box.

Any technicians who need elevated access (admin rights) to VIU systems or servers, please ensure they sign a copy of page 2 ELUP Terms and Conditions.

All technicians must read and comply with the VIU **Use of Information Technology Policy** 45.01 (note: Policy 45.01 is under review and a new version will be sent when completed).

| Use Page 1 access | Tech First and Last Name | Tech Email address | Tech Phone # | Special Access requirements | ELUP? |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

VANCOUVER ISLAND UNIVERSITY

# Policy 45.01
# Use of Information Technology

| | | | |
|---|---|---|---|
| **Type:** | C - Institutional | **Last Approved:** | Oct. 21, 2009 |
| **Executive Responsibility:** | Vice-President Administration & Finance | **Next Review:** | Mar, 2010 |
| **Administrative Responsibility:** | Director, Information Technology Services | **Procedure:** | 45.01.001<br>45.01.002 |

1. GENERAL POLICY STATEMENT

1.1 Vancouver Island University provides information technology resources to employees, students, and associates in order to further the teaching, learning, research, and administrative purposes of the institution. In certain situations, such as the Library, limited opportunities to use information technology resources may also be extended to members of the public. For the purpose of access to information technology, the definitions of "associate" and the requirements for status as an associate can be found in Procedure 45.01.001, "Access to Information Technology – Associate Privileges".

1.2 Under this policy, the University Executive may, from time to time, authorize standards, regulations and guidelines to ensure that information technology is used efficiently and appropriately. (see Section 6 below).

1.3 All users of information technology at Vancouver Island University must abide by this policy and any related rules and standards or risk loss of access to information technology and other penalties.

2. INFORMATION TECHNOLOGY DEFINED

2.1 Information technology encompasses all computing and communications facilities and services provided by Vancouver Island University, including voice-mail and telephone service, computers, networks, accounts and storage, software, web pages and websites, and Internet access. It also encompasses services (for example, websites) hosted elsewhere when they are operated on behalf of the University.

2.2 As an organizational area within the University, "information technology" includes the library, education technology, and institutional research, as well as the units directly responsible for information systems, network administration, and computer support. The responsibilities in this Policy that are linked to the "Director, Information Technology" can be executed by a Director of any one of these more specific services or by the Vice-President Administration and Finance.

3. CONFIDENTIALITY, SECURITY, AND THEIR LIMITS

3.1 Privacy and confidentiality are important values for Vancouver Island University. Normally, users can expect that their communications and the contents of their accounts will be treated as private and confidential and that their files will not be accessed without their permission. However, individuals have no right to absolute privacy when using information technology atVancouver Island University. The University owns the information technology infrastructure and is responsible for its use. The University reserves the right to take action to see that its information technology is used lawfully, appropriately, and efficiently in pursuit of the primary purposes of the institution.

3.2 Privacy does not extend to the following situations:

3.2.1 Aggregate statistics about user accounts are not confidential (for example, data that indicate the amount of storage being used by particular accounts for .jpg files).

3.2.2 As a normal part of system administration, information technology employees monitor levels of network traffic, use software that logs network activity, make copies of files, and maintain archives of these copies.

3.2.3 Information technology employees may access any file, data, program, or e-mail in order to gather sufficient information to diagnose and correct network, hardware, and software problems. (see, also, the obligations of information technology employees in Section 5.1, below).

3.2.4 Information technology employees will compile and release otherwise confidential information when this is requested in accordance with Section 3.3 of this Policy.

3.3 The University information technology staff will gather and release information that is normally confidential only when specifically requested to do so and only when the request meets the following three conditions:

3.3.1 The request is made by the appropriate office in the institution. These offices are:

- Human Resources or Health and Safety Services with respect to compliance with WorkSafeBC legislation.
- The Executive Director, Communications & Public Relations (or another person authorized by the President to execute the legal obligations of the University with respect to legislation concerning freedom of information and protection of privacy) with respect to Freedom of Information requests or requests from law enforcement agencies for assistance with investigations.
- The Executive Director, Student Services (in the case of students) or the Human Resources Department (in the case of employees and associates) with respect to an internal University investigation.

3.3.2 The request is made in writing, is reasonably specific in terms of the information required, and specifies to whom the information is to be released. (The request to the Director, Information Technology to gather and release information need not contain reasons why the information is required. The person and office issuing the request according to Section 3.3.1 has the obligation to establish and document these reasons and to ensure that the request and subsequent actions comply with the appropriate laws and policies under which they are acting.)

3.3.3 The request is addressed to the Director, Information Technology who shall be responsible for fulfilling the request, even though the actual work of gathering the requested information may involve other information technology employees.

3.4 The University does not guarantee the security of any messages or files sent or received through its networks. Although the University will employ various tools and methods to enhance network security, all users need to be aware that others can potentially intercept or accidentally receive data sent over a computer network.

3.5 The University assumes no liability for files and information that are stored on its systems. It has no obligation to maintain or destroy any or all physical representations of particular files.

4. OBLIGATIONS OF USERS

4.1. Legal Use

4.1.1 Vancouver Island University requires all employees, students, associates and members of the public to use its information technology resources in ways that uphold all federal, provincial, and local laws and regulations. Areas of particular concern include:

- The Criminal Code of Canada. Threats, harassment, or others crimes committed electronically are crimes.
- Copyright Act. Storing, using, or displaying programs, images, or data without the proper permissions is theft.
- Freedom of Information and Protection of Privacy Act. Information in an e-mail or on a website can easily be distributed beyond the intended audience and thereby infringe someone's right to privacy.
- Human Rights Code. All material that becomes public must respect the right of people to live in an atmosphere free of hatred, contempt, or discrimination. For example, it is illegal to display or print sexually explicit or racist material in a computer lab or in any other public context where others are likely to see it.
- WorkSafeBC legislation. The obligation to maintain a safe and healthy working environment is a broad one and includes specific requirements concerning workplace violence, threats, and discrimination.

4.2. Acceptable Use

4.2.1 Users of information technology are required to meet expectations and standards of professional and ethical behavior that go beyond the requirements of law. These standards and expectation of "acceptable use" are designed to help achieve both (i) a positive learning and working environment in which all persons treat each other with dignity and respect and (ii) the effective and efficient operation of information technology resources.

4.2.2 The requirements and expectations of acceptable use are contained in University policies, guidelines, and collective agreements and in the rules and standards that may from time to time be issued under the authority of this Policy, Section 6.

4.3. Using information technology for non-University business

4.3.1 Occasional and incidental use of e-mail, voice mail, and Internet access for personal purposes is acceptable, provided that these uses, in the opinion of the University, do not:

- Interfere with institutional business (i.e., teaching, learning, research, and administration);
- Detract from an employee's availability to carry out his or her assigned responsibilities;
- Damage the University's reputation; and
- Compromise the integrity and efficiency of the institution's information technology facilities and services.

4.3.2 Except in the case of *InVIU* where free access and use of resources is permitted, use of University information technology and resources for commercial purposes or for the benefit of organizations not directly affiliated with the University is forbidden without the written consent of the Vice-President Administration and Finance. This includes, but is not limited to: any advertising on web pages or via e-mail or news postings; any solicitation of funds, goods, or services for any purpose; and processing or transmission of data on behalf of a third party whether a fee is charged or not.

4.3.3 All personal and approved commercial use of information technology resources has the same status as institutional use and is subject to the same expectations regarding legal and acceptable use.

4.4. Reporting possible illegal and unacceptable use

4.4.1 Employees should report to their supervisor all suspected illegal or unacceptable use of information technology resources.

4.4.2 Deans and Directors shall forward reports of possible illegal or unacceptable use to either the Executive Director, Student Services (in the case students) or the Human Resources Department (in the case of employees and associates). In the interests of efficiency, instructors can (in the case of students in their classes)

report cases of possible illegal or unacceptable use of information technology directly to the Executive Director, Student Services, with a copy to the Dean of their Faculty.

5. OBLIGATIONS AND AUTHORITY OF INFORMATION TECHNOLOGY STAFF

5.1 Like all other members of the University community, employees who support the information technology infrastructure and provide information technology services are expected in the normal course of business to use information technology appropriately, respect the privacy of others, and maintain the confidentiality of information that may come to their attention during the routine exercise of their duties.

5.2 Information technology employees will ascertain and release information that is normally confidential only when specifically requested to do so according to the provisions of Section 3.3 of this Policy.

5.3 In situations where there is an immediate threat to the integrity and availability of the University's networks and data systems, technicians and administrators in information technology have the obligation and authority to take the measures that they, in their professional judgment, think are necessary to secure the networks and systems for general use, even if this means denying access and causing loss or inconvenience to some users.

6. ISSUING RULES AND STANDARDS

6.1. In order to promote a positive working and learning environment and to ensure that limited information technology resources are used effectively and efficiently, this Policy envisages additional rules and standards on a wide variety of topics related to information technology—for example: standards for equipment that is to be connected to the network; quotas on network storage; and expectations for e-mail etiquette.

6.2 The process for authorizing rules and standards under this Policy shall include the following steps:

- A proposal is advanced by a member of senior management (i.e., a Dean, Director, or Principal).
- There is adequate time for the Director, Information Technology or Vice-President Administration and Finance to evaluate the proposal and make recommendations.
- The proposal is considered by Management Committee, and possibly by others, before it is revised and forwarded to the Executive.
- The Executive makes a final decision on the rules or standards, and the President authorizes these.
- The existence of the new or changed rules and standards is communicated broadly to employees and students by whatever methods seems appropriate—for example, by e-mail, splash screens, and/or web postings.

6.3 Rules and standards approved according to Section 6.2 shall be documented as Procedures under this Policy.

## 7. SANCTIONS AND PROCEDURES IN CASES OF ALLEGED MISUSE

### 7.1 Investigating alleged misuse of information technology

7.1.1 The University may undertake investigations of specific allegations of alleged misuse of information technology. These investigations may involve the collection and analysis of information that is otherwise considered private and confidential, subject to Sections 7.1.2 and 3.3 of this Policy. The University will not engage in investigations without probable cause.

7.1.2 In the case of students or members of the general public, only Executive Director, Student Services may authorize investigations of alleged misuse of information technology. In the case of employees and associates, only the Human Resources Department may authorize an investigation. In cases where the identity of the person of interest is unknown, either the Executive Director, Student Services or the Human Resources Department may authorize the investigation, but the further conduct of the investigation will fall to the appropriate person once the identity is known. All investigations must comply with the Policy provisions under which they are conducted—for example, notifying people that their actions are under investigation and ensuring appropriate levels of confidentiality.

### 7.2 Processes for cases of alleged misuse

7.2.1 Within the University, the processes used to consider cases of alleged misuse of information technology will be those normally used for cases involving possible student or employee misconduct. Sanctions will include those allowed under various University policies, procedures, and collective agreements.

7.2.2 In addition to other sanctions, misuse of information technology may result in denial of access to the technology or specific limitations on its use. Any such denial or restriction must be reasonable in terms of time limits and extent.

7.2.3 The Executive Director, Student Services and the Human Resources Department have the authority to order the temporary withdrawal or limitation of privileges to use information technology pending a fuller investigation of alleged misuse.