

# *NC Curriculum:*

---

## **Network Contact Responsibilities and Procedures Manual**

# Contents

<b>Network Contact Requirements .....</b>	<b>1</b>
Minimum Departmental Requirements .....	1
Network Contact 1 .....	1
Description of Duties .....	1
Responsibilities include .....	1
Required Knowledge and Skills .....	1
Required Training .....	1
Additional Information .....	1
Network Contact 2 .....	2
Description of Duties .....	2
Responsibilities include: .....	2
Required Training .....	2
Required Knowledge and Skills .....	2
<b>Definitions .....</b>	<b>3</b>
Network Contact.....	3
OHSU Workstation .....	3
The OHSU Network.....	3
OHSU Services .....	4
ITG Help desk.....	5
Computer Access Administration .....	5
Employee Training.....	5
Volume Licensing.....	5
ITG Help desk Staff Meetings.....	5
Departmental Applications.....	6
Local Applications.....	6
<b>Procedures.....</b>	<b>7</b>
Problem Resolution .....	7
Basic Troubleshooting .....	7
Problem Ticket Priorities – <i>Brief Description</i> .....	8
Problem Ticket Priorities – <i>Full Description</i> .....	8
Requesting User Network Accounts .....	9
Requesting Info Retrieval from another User's Account .....	10
Reporting Network Contact Changes .....	10
Requesting a Public Network Subdirectory.....	10
Requesting a GroupWise Resource.....	11
Requesting a GroupWise Generic E-mail Account.....	11
Requesting a Listserv.....	11
Requesting a GroupWise Public Group.....	12
Requesting a J-Drive.....	12
Projects.....	12
FTS Project Request .....	12
ITG Project Request .....	13
<b>Security Policies.....</b>	<b>14</b>
INFORMATION SECURITY AT OHSU....	15
<b>Methods of Communication .....</b>	<b>22</b>
Network Contact E-mail .....	22
Network Contact Meetings .....	22
NC Forums .....	22
User Groups .....	22
<b>Curriculum .....</b>	<b>23</b>
Employee Training.....	23
TrainingForce .....	23
NC Program Duties and Required Training .....	23
Network Contact Curriculum .....	24
Class Descriptions: Network Contact Curriculum For up-to-date Network Contact class schedule and class descriptions go to: <a href="http://www.ohsu.edu/etc/classes/schedule.shtml">http://www.ohsu.edu/etc/classes/schedule.shtml</a> .....	24

Suggested End User Curriculum .....	24
Class Descriptions: End User Curriculum .....	25
For up-to-date IT Training class schedule and class descriptions go to: <a href="http://www.ohsu.edu/etc/classes/schedule.shtml">http://www.ohsu.edu/etc/classes/schedule.shtml</a>	25
Computer Proficiency Licenses .....	25
<b>Appendix – Resources .....</b>	<b>26</b>
Computer Skills Checklist .....	27
NC Web Sites .....	28
OHSU Drive Definitions and Usage for PCs .....	30
ACCEPTABLE USE OF COMPUTING AND TELECOMMUNICATIONS RESOURCES .....	31
<b>Software Management Guide .....</b>	<b>36</b>
<b>Software Log .....</b>	<b>40</b>

# Network Contact Requirements

The Network Contact, or “NC”, functions as a single point of contact between their local department and Information Technology Group (ITG). The role of the NC has evolved over time and functions as a troubleshooter, problem solver and communicator. This role is vital in supporting and maintaining the business and computing function of the University.

## Minimum Departmental Requirements

- One primary NC or TC per department/shift or per minimum of 15-20 co-workers
- One back-up NC or TC per department/shift or per minimum of 15-20 co-workers
- Must be a permanent employee (Temporary Employee/Student is not eligible)
- NEW – Must be employed by OHSU for at least six months (knowledgeable about OHSU Policies/Processes)
- Must have department manager approval
- Departments with less than 15 people should have a primary NC and one back up NC

## Network Contact 1

### Description of Duties

The Network Contact 1 (NC 1) assignment will be reserved for NCs with windows and mouse skills, knowledge of GroupWise, knowledge of web-browsing, an understanding of purchasing processes and good communication skills.

### Responsibilities include

- ✓ Single point of contact (SPOC) for submission of network projects and problems
- ✓ Coordination between ITG and their Department for completion of projects
- ✓ Provide relevant or pertinent information from ITG to department managers and co-workers
- ✓ Attend the monthly NC meeting or watch streaming video of meetings
- ✓ Responsibilities at this level will not include any software/hardware troubleshooting
- ✓ Pass along relevant (or pertinent) information from ITG to co-workers

These NC duties may fall within an existing position description as “other duties as assigned”.

### Required Knowledge and Skills

- Windows and mouse skills (basic Macintosh and mouse skills for NCs supporting MACs)
- Knowledge of GroupWise
- Knowledge of web-browsing and online forms submission
- Understanding of purchasing processes
- Good communication skills

### Required Training

See information in curriculum section of this manual.

### Additional Information

An NC 1 may move to an NC 2 by taking the currently advanced NC classes after they take the orientation class. Your NC 1 status will then be changed to NC 2.

# Network Contact 2

## Description of Duties

In addition to the duties of the Network Contact 1, the NC 2 is required to have an intermediate level of computer knowledge to provide basic hardware and software troubleshooting.

## Responsibilities include:

- ✓ Network Contact 1 Responsibilities; PLUS
- ✓ Provides front-line hardware and software troubleshooting support
- ✓ Have a basic knowledge of all current core applications used by your department
- ✓ Completion of the training listed in the Required NC Training Classes chart located in the NC Curriculum section.
- ✓ Assists departmental staff in reporting security incidents. See “Reporting Security Incidents” (<http://www.ohsu.edu/ohsuedu/central/itg/about/policies.cfm>)
- ✓ OPTIONAL: NEW – Assists manager with budgeting software/hardware purchases
- ✓ OPTIONAL: NEW – Manages computer equipment inventory, including surplus of out-of-warranty equipment (may require Excel knowledge; provide downloadable Excel equipment inventory form on NC/TC Resources web page).
- ✓ OPTIONAL: NEW – Manages software purchases/licensing (may require excel knowledge; provide downloadable Excel software inventory form on NC/TC Resources web page)
- ✓ OPTIONAL: NEW – Assesses departmental staff computer training needs and assists scheduling them for the appropriate classes.
- ✓ OPTIONAL: NEW – Wireless configurations

## Required Training

See Required NC Training requirements located in the Curriculum section of this manual.

## Required Knowledge and Skills

- ✓ Network Contact 1 Requirements; PLUS
- ✓ Knowledge of applications used in department
- ✓ Basic hardware setup experience
- ✓ Basic troubleshooting skills

# Definitions

## Network Contact

There is a wide spectrum of NCs in our community. They range from the single point of contact who only report problems to ITG, NC 1's, to the troubleshooter who tries to resolve problems, NC 2's. **The department management is responsible for determining the level of service and knowledge it requires from the NC.**

As described, ITG has outlined specific policies and procedures to help the NC better serve their department and to aid ITG in better serving them. In addition, the NC has the opportunity to learn about the network and how to troubleshoot problems by taking classes offered by IT Training.

## OHSU Workstation

The **OHSU Workstation** is the name given to the common set of standards and programs. It delivers OHSU information systems services in a consistent fashion throughout our campus and outreach communities. The main aims are to:

- Maintain network wide standards for supported utilities and applications
- Choose those standards which best provide current and future compatibility with other systems and provide a base on which to build future services.
- Where possible, provide access to network resources independent of location or platform type.
- Provide improved services to all network users while maximizing use of network hardware already deployed.

The OHSU Workstation will deliver the following functionality to Windows and Macintosh computers:

- A standard network operating system providing file and print services.
- An integrated electronic mail, calendar-scheduling and workflow system.
- Access to OHSU information systems.
- Access to OHSU's Intranet and world wide web.

## The OHSU Network

OHSU features an extensive network of computing resources and integrated network of over 9,000 workstations. Typically, academic medical centers have separate networks to support their clinical, research and academic environments. OHSU clinicians, students, faculty and staff have access to a set of standard features from everywhere on the network. Personnel may access the network from Macintosh or PC desktop workstations. Students may access the campus network from the OHSU Main Library and branches, in computer labs and classrooms, and via the Internet or modem.

Each network user has a directory on the network for storing personal electronic files. In addition, group directories are provided for each department to store shared documents. Access to a variety of printers is also available when logged into the network.

# OHSU Services

OHSU services are the applications provided by ITG at no charge to the departments or users. They are updated as new software releases are available and tested. These applications are fully supported and training is available through OHSU.

The Network Contact 2 will be the **first contact** for all end users in regarding OHSU services.

Some services, such as Oracle, TPS, Ovid, and GroupWise, require a login and password to access the application.

- GroupWise
  - Electronic Mail
  - Calendaring/Scheduling
  - Task Routing
- Windows/Macintosh versions of Microsoft Office
  - Word
  - Excel
  - PowerPoint
  - Access (not available on Macintosh computers)
- Administrative Tools
  - Various computer tools
- Internet Access
  - FTP
  - Internet Explorer
  - Ping
  - Telnet
- Network Associates
  - Virus tools
- Reference Services
  - Library Catalog
  - Ovid
  - Micromedex
- Administrative Services
  - ASIP Logon (Financials)
  - Human Resources Information System
  - Student Information Services (SIS)
  - Time and Attendance (Kronos)
- Patient Services
  - Radiology Systems
  - Pharmacy Systems
  - A2K or Mainframe Access to Clinical Systems
  - Other Host Systems
- Policies and Procedures
  - Hospital Policies and Procedures
  - University Policies and Procedures
  - Health Care System Policies and Procedures

## ITG Help desk

The ITG Help desk is the communications link between the network users and the network infrastructure.

ITG Help desk analysts help Network Contacts and other customers solve or escalate hardware problems, software problems, obtain and modify user accounts, perform password resets, and communicate changes in network services (upgrades, downtimes).

Full ITG Help desk support is available Monday through Friday, 6 am to 6 pm by calling 494-2222. Non-urgent questions and issues can be communicated by e-mail to [helpdesk@ohsu.edu](mailto:helpdesk@ohsu.edu).

After-hours support is provided by ITG Computer Operations M-F 6 pm - 6 am and 24 hours on weekends. They can be reached by calling 494-2222, the same number for the ITG Help desk. Computer Operators are not trained to provide full ITG Help desk support, but they can:

- Refer critical patient care and e-mail issues to appropriate on-call personnel if necessary
- Reset passwords.

Customers should call the ITG Help desk for assistance before calling other ITG staff directly, unless specifically instructed. This enables ITG to balance workloads, track trends, and ensure reliable, consistent support.

## Computer Access Administration

Computer Access Administration requests are for administrative adds or changes to the network. Some of the more common administrative requests are:

- New user (needs network sign-on)
- Change to existing sign-on (for any system, e.g. network, SMS, Lab)
- Deletion of a user (30 days after person left department)
- Transfer of a user (from one department to another)
- Name changes

## Employee Training

Employee training includes courses on Desktop Applications, Healthcare Applications, Oracle Applications, Library Applications, etc. The OHSU Employee Learning Portal is at: [www.ohsu.edu/learning](http://www.ohsu.edu/learning) This is an ever-growing portal.

## Volume Licensing

Volume Licensing Program policies and procedures must be followed. The Web site containing information is: [www.ohsu.edu/library/software/](http://www.ohsu.edu/library/software/)

## ITG Help desk Staff Meetings

The **ITG Help desk** staff meets every Tuesday from 11:30 am to 1:00 PM. Minimal phone coverage is provided. However, there may be longer hold times; please be patient. If a problem can wait, please call after 1:00 PM.

## Departmental Applications

Applications that reside on the network for use by multiple people within one or more departments, but are not utilized across the entire network. Applications that are approved by agreement with ITG and the department will be loaded on the network with the assistance of ITG and the Network Contact.

It may be the NC's responsibility to provide support for departmental applications. The ITG Help desk can only support access to departmental applications. Feature support will not be provided by the ITG Help Desk.

If the problem with the departmental application is due to a network or workstation (can't get into the application or can't print from the application) problem, ITG will assist you. Please be prepared to explain how you have determined that this is a network or workstation problem.

## Local Applications

If you want to load an application on your networked workstation, and you have problems, read the manuals and call the software vendor for help before calling the ITG Help desk.

Assistance will not be granted from the ITG Help desk or technician without evidence of a license.

# Procedures

## Problem Resolution

The ITG Help desk is the primary resource for Network Contacts trying to resolve hardware, software, or network connectivity issues. Problems which need to be resolved as soon as possible should be submitted by phone to 494-2222. If the Help desk analyst cannot solve your problem while you are on the phone, he or she will open a ticket and assign the problem to the appropriate resource for resolution. The NC is responsible for tracking that problem ticket to resolution. Be sure to get the problem number for any call which isn't resolved immediately.

Problem tickets entered into the database are tracked by ITG. Analysis of this data assists in decisions regarding staffing and infrastructure throughout OHSU.

Problems that are not urgent may be e-mailed to [helpdesk@ohsu.edu](mailto:helpdesk@ohsu.edu). You will receive an automated response acknowledging receipt, and you may expect a 48-hour turnaround time for response from an analyst.

## Basic Troubleshooting

A few basic steps will solve many problems. They are:

1. Check and make sure the cords are plugged tightly into the machine. A suggestion is to unplug and plug in the cords.
2. Write down any error messages.
3. Unless you are worrying about losing a file that you were working on and had not saved, reboot the computer.

If the problem is not solved then call the ITG Help desk. Be prepared to give the information as listed below.

Please provide as much of the following information, as possible:

- NC Full Name
- Department
- Device ID (three letters and four numbers, *e.g.* BIC0267, or inventory number)
- NC's Phone Number
- User's Full Name and Phone (if you are calling for someone else):
- Login ID
- Server and/or Context of user and device
- Device Type
- Location (building and room)
- Problem
  - When problem started (best guess)
  - What was the user trying to do
  - What you've done to troubleshoot the problem
- How urgently you need resolution
- Any additional information you feel will help the analyst direct the problem to the appropriate resource

## Problem Ticket Priorities – *Brief Description*

PRIORITY 1: 911 – Patient Care - ***Applies to Hospitals and Clinics only.***

PRIORITY 2: Urgent – Mission critical for customer and an urgent need for technical assistance.

PRIORITY 3: Normal – Acceptable workaround is available.

PRIORITY 4: Maintenance – Downgraded support.

## Problem Ticket Priorities – Full Description

<i>Priority</i>	<i>Response Time*</i>	<i>Max time to Resolution*</i>
<b>Priority 1</b> 911/Patient Care (Applicable only to FTHC Zone)  Direct Patient Care is affected	Call back from FTS within 15 minutes and immediate service	12 hours
<b>Priority 2</b> Urgent/Mission Critical  Enterprise Business app is affected	Call back from FTS within 30 minutes and remote or on-site service within 1 hour	12 hours
<b>Priority 3</b> Normal	Call back from FTS within 4 hours and remote or on-site service within 48 hours	10 business days
<b>Priority 4</b> Maintenance	Call back within 48 hours and remote or on-site service within 21 business days	28 business days
* These response and resolution times are for FTS support and do not include additional time required by a vendor or other ITG departments if an issue requires escalation.		

## Requesting User Network Accounts

All requests for these services are submitted by accessing the Network Services Usage Agreement form, , which is found at <http://helpdesk>

1. Select **Computer Access** on the left side navigation bar
2. Make appropriate selection
3. Read the OHSU user policy at [http://ozone.ohsu.edu/policy/pac/chapt\\_11/11-20-010.htm](http://ozone.ohsu.edu/policy/pac/chapt_11/11-20-010.htm).
4. **Select the appropriate user access needed in the “OHSU Access” section and complete the form.**

## Requesting Info Retrieval from another User's Account

There are times when a department must request access to a specific file, directory or for information to be retrieved from a user's e-mail account.

1. The chair, director or head of the department must submit a request for access to specific file or directory or for information to be retrieved from user e-mail to the OHSU Information Security Officer through Computer Access at [logins@ohsu.edu](mailto:logins@ohsu.edu)
  - a. Specific information to be retrieved; reason for and circumstances of the request, name and login id of the person whose information is being requested; name and login id of the person who should be given access to this information, timeline for this request (is it urgent or at convenience?)
2. The request will be forwarded to the Chief Information Officer and the Director of Human Resources for approval and implementation by the Information Security Officer or, if deemed necessary, the request will be referred to the appropriate executive for approval.
3. Access to information, if approved, will be granted for a limited duration after which, access will be removed. If access to files or directories is granted, the receiving party will be given a copy of the materials and the original versions will remain as the owner left them.

*This information access policy is not intended for use by departments who may want to gather information about personnel use and misuse of the network services, nor is it intended to be used as a tool for supervision of employees or to attempt to enforce department use policies. Such requests will be disallowed*

*Note: It is recommended that departments make arrangements to transfer files to shared space in preparation for a change in personnel and prior to the departure of the files owner.*

For more information please review the Technical Directive for Access to Private Files, Data, and E-mail at <http://ozone.ohsu.edu/itg/policies/td/td139801.shtml>.

## Reporting Network Contact Changes

Any time there is a change in the status of the NC in your department fill out the NC Changes form on the web at: <http://www.ohsu.edu/etc/forms/nc-update.shtml>

## Requesting a Public Network Subdirectory

Departments who distribute documents organization-wide may request access to a public network subdirectory. Departments must agree to follow public directory policies and procedures. Instructions to request access, plus policies and procedures are located on SHR on Share1: i:\ohsu\public\public.doc.

## Requesting a GroupWise Resource

A resource is an object in GroupWise that can be scheduled. Examples of resources are conference rooms, departmental calendars or departmental equipment. See the following examples:

RESOURCE NAME	RESOURCE DESCRIPTION	RESOURCE OWNER
BICC 123	Conference Room	Skye Leslie
IT Training	BICC Training Room Schedule	Susan Conrad
ITG Out	Department use for employee leave codes	Terri Butler

To request a GroupWise Resource, go to: <http://ozone.ohsu.edu/itg/cacc/resource.shtml> and after you enter the appropriate information submit the form.

## Requesting a GroupWise Generic E-mail Account

Departments who use e-mail to communicate general departmental information with their external customers can set up a generic e-mail account. An example of a generic e-mail account is [helpdesk@ohsu.edu](mailto:helpdesk@ohsu.edu). Rather than communicate with an individual analyst, customers can send their questions to a generic account that is frequently monitored by all appropriate staff within the department.

Many requests that come into Computer Access are for access to individual e-mail accounts because the employee had to go on leave, and they were conducting official departmental business from their own personal account. By setting up a generic account for the department, this is avoided.

Additionally, Web Services requires that contact information be included in the "address" section of all web pages that are posted. ITG recommends that you never post a personal e-mail account, but rather, you maintain a departmental generic account for such purposes.

To request a GroupWise Generic E-mail Account, go to: <http://ozone.ohsu.edu/itg/cacc/generic.shtml> and after you enter the appropriate information submit the form.

## Requesting a Listserv

A Listserv is an e-mail account that reaches a large audience of people interested in the same topic.

**Note: Listservs are self-maintained after the initial set-up.**

To request a Listserv go to: <http://ozone.ohsu.edu/itg/cacc/majordomo.shtml> and after you enter the appropriate information submit the form.

## Requesting a GroupWise Public Group

A public group is used for sending unsolicited email to more than 50 people at any given time. It must be approved by University News and Publications first.

**Note: GroupWise Public Groups must be maintained by ITG.**

To request a GroupWise Public Group go to: <http://ozone.ohsu.edu/itg/cacc/generic.shtml> and follow the instructions listed.

## Requesting a J-Drive

The j-drive is an additional departmental shared drive that can be configured to include/exclude certain staff; e.g. staff that may not be involved with a program.

To request a j-drive, use the **ITG Project Request** form at <http://istart/request/new/login.cfm?return=/request/new/index.cfm> and follow the instructions listed. If you have not already created a user name or password in the IT Project Request Manager, you will be prompted to do that.

## Projects

### FTS Project Request

Includes workstation/printer moves, installs and hardware upgrades on the network. If you do not know if you have an FTS Project to submit, please call the Computer and Phone Services (CAPS) Office at 494-4622, who will assist you in your decision.

#### FTS Project Submission:

- To submit a request go to the CAPS Website at [http://helpdesk/viewindex.aspx?key\\_id=1376](http://helpdesk/viewindex.aspx?key_id=1376). For telephone related services go to [http://helpdesk.ohsu.edu/viewindex.aspx?key\\_id=1385](http://helpdesk.ohsu.edu/viewindex.aspx?key_id=1385). You have an option of filling out a Computer Only or combined Phone/Computer request form. Anticipate that you will be **required at minimum** to provide the following information:
- Include the following information:
  - Department
  - Building(s) & Room Number(s)
  - Contact for this project
  - Requested Completion Date
  - PC Type, i.e., Macintosh/Intel or Printer Type
  - Is this a new install or a replacement? (If replacement, give terminal ID's)
  - Do you wish to have ITG process a PO for new equipment?
  - Please detail what equipment you would like to have ordered?
  - Scope of this project (individual or a group - if group indicate number)
  - Nature of Project (be as precise as possible)
  - Workstation(s) Terminal ID(s) involved (New installs will not have this)
  - Printer(s) ID(s) involved (New installs will not have this)
  - Account number **ALIAS** to bill any applicable computer related equipment to
  - Name of Fiscal Authority over the above account number(s)
  - Can the Fiscal Authority approve Purchase Requisitions in the online Oracle System
  - What is the Oracle Hierarchy of the fiscal authority

Upon receipt, your request will be assigned to an FTS member in your zone. The project request will be reviewed and a priority will be assigned. As a general rule, projects are completed on a “first in, first out” basis, with adjustments made based on Client input, equipment availability, and technician resources.

## **ITG Project Request**

All requests for ITG services, except for telephone and computer workstation/printer moves, installs and hardware upgrades on the network. If you do not know if you have an ITG Project to submit, please call the *ITG Help desk* at 494-2222.

### **ITG Project Submission Instructions:**

1. Go to the ITG Help desk website
2. Select **IT Request Manager** from the Left Navigation panel
3. First timers: Go to **Need an account?** and click on “Click here to sign up”

# Security Policies

Access to private files, data, and e-mail is controlled Office of Integrity: Office of Privacy and Security at: <http://www.ohsu.edu/cc/hipaa/forms.shtml> and <http://ozone.ohsu.edu/cc/hipaa/policy.shtml>.

- Expectation of Privacy:
  - User's H-drive file space; this is a private drive space for OHSU documents
  - University computing resources are not private. For example, communications made by means of University computing resources are subject to Oregon's Public Records Law to the same extent as they would be if made on paper. As agreed to by each individual user on the OHSU network (by signing the NC04.wpd), no user is authorized to login with any login ID other than the one assigned to them personally.
- No user is permitted to authorize access with their personal login ID by anyone else under any circumstances.
- *Departments are encouraged to keep shared files and other mission critical files on the shared drive rather than within an individual user's file storage.*
- ITG recognizes that there are some circumstances, which may necessitate access to another user's directories or files.
  - If a user vacates a job suddenly due to illness or death
  - If a user leaves employment suddenly and has department files which are mission critical
  - If there is evidence of misuse or other violations of the acceptable Use Policy
- E-mail access is a special case which involves issues of privacy and confidentiality for the owner of the e-mail account as well as any and all correspondents who may have sent e-mail to the owner.
- Certain types of correspondence which are particularly sensitive may include:
  - Correspondence containing patient data
  - Correspondence referring to proprietary research
  - Correspondence which may give evidence of employee's performance and other personnel issues

Therefore, ITG will not grant direct access into E-mail, but may, under certain circumstances and with special authorization, search E-mail for correspondence pertinent to a specific topic or issue and provide pertinent information to the requesting party.

This information access policy is not intended for use by departments who may want to gather information about personnel use and misuse of the network services, nor is it intended to be used as a tool for supervision of employees or to attempt to enforce departmental use policies. Such requests will be disallowed.

# INFORMATION SECURITY AT OHSU....

Slide 1



---

---

---

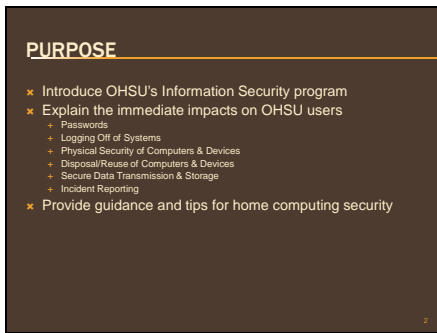
---

---

---

---

Slide 2



---

---

---

---

---

---

---

Slide 3

**OVERVIEW**

- ✦ HIPAA Security Rule (effective date April 20<sup>th</sup>, 2005)
- ✦ Good business practices (not just a HIPAA requirement)
  - + Confidentiality (per the HIPAA Privacy Rule)
  - + Availability
  - + Integrity
- ✦ Covers all "restricted" information, all information systems, and the entire OHSU workforce
- ✦ Reasonable and appropriate

---

---

---

---

---

---

---

---

Slide 4

**OHSU INFORMATION SECURITY RULES**

- ✦ Establishes Information Classifications
  - Classified
  - Confidential
  - Proprietary
  - + Public
  - "Restricted" Information
- ✦ Assigns Responsibilities for
  - + Users
  - + Stewards
  - + Managers
  - + Service Providers
  - + Information Security Officer
  - + And more...

---

---

---

---

---

---

---

---

Slide 5

**USER RESPONSIBILITIES**

- Familiarity with and adherence to OHSU policies
- Physical security
- Secure storage of information
- Secure distribution and transmission of information
- Appropriate destruction and disposal of information and devices
- Access Control and Authentication
- Computer Security
- Use of appropriate remote access systems
- Logging out or Securing sessions
- Contingency Planning

---

---

---

---

---

---

---

---

Slide 6

**UNACCEPTABLE USE**

Unacceptable use includes but is not limited to:

- + Breach of a person's or patient's privacy and confidentiality
- + Shared log-ins
- + Copyright and/or trademark infringement
- + Accessing pornography
- + Download movies or MP3's for personal purposes
- + "Hacking," "cracking," and similar activities
- + Breach of OHSU's sexual harassment policy
- + Violation of any and all applicable software licenses
- + Text messaging health information beyond the minimum information necessary for a treatment purpose.
- + All broadcast e-mails (>50 addresses) must be submitted and approved by UNP

---

---

---

---

---

---

---

---

Slide 7

**PASSWORD STANDARDS**

- \* "Complex" passwords required
  - + 6 character minimum
  - + Must include the following
    - \* Alpha (abc...)
    - \* Numeric (123...)
    - \* Symbol or punctuation (!@#\$...)
- \* Must change every 180 days
- \* No writing down passwords
- \* No sharing passwords

---

---

---

---

---

---

---

---

Slide 8

**LOGGING OFF ELECTRONIC SESSIONS**

- \* Users will secure computing device sessions when leaving devices unattended
- \* Automated "inactivity" logoffs/locks (e.g. screensavers) required after:
  - + 10 minutes for devices accessing restricted information
  - + 3 minutes for shared clinical workstations
  - + 30 minutes for applications/databases that store or access restricted information
- \* Systems that cannot (technically) comply shall implement procedural and physical controls to compensate.

---

---

---

---

---

---

---

---

Slide 9

**PHYSICAL SECURITY OF COMPUTERS & DEVICES**

- ✦ Physical access to a device can bypass virtually all technical controls (e.g. passwords)
- ✦ Portable Devices + Insecure Areas = **HIGH RISK**
- ✦ Requirements for physical security of the devices are based on
  - + Type of device
  - + Sensitivity of data
  - + Location of device

---

---

---

---

---

---

---

---

Slide 10

**DISPOSAL/REUSE OF COMPUTERS & DEVICES**

- ✦ Restricted information shows up everywhere and on virtually every computer device at OHSU
- ✦ Devices may be recycled to anyone within OHSU and donated to any number of external agencies (e.g. schools)
- ✦ We have a requirement to ensure that the restricted information is "unrecoverable" prior to disposing or recycling of devices

---

---

---

---

---

---

---

---

Slide 11

**DISPOSAL/REUSE OF COMPUTERS & DEVICES**

- ✦ OHSU computers/devices – submit request to ITG
  - + Disposal - [http://helpdesk.viewer.aspx?key\\_id=1711](http://helpdesk.viewer.aspx?key_id=1711)
  - + Reuse - [http://ozone.ohsu.edu/itg/caps/computer\\_form.shtml](http://ozone.ohsu.edu/itg/caps/computer_form.shtml)
- ✦ Non-OHSU devices – follow the sanitization guidelines at <http://ozone.ohsu.edu/cc/sec/isg/>
- ✦ Make sure you backup any important information prior to disposal.

---

---

---

---

---

---

---

---

Slide 12

**SECURE DATA TRANSMISSION & STORAGE**

- ✦ Concept: *trusted* versus *un-trusted* systems
- ✦ Restricted information on *trusted* systems
  - + Encryption is not required (unless specified elsewhere)
  - + Information should be stored based on authorized users (departmental shares, restricted folders, etc.)
- ✦ Restricted information on *un-trusted* systems
  - + Encrypted
  - or
  - + Password-protected
  - or
  - + Patient individual consent (individual-specific)
- ✦ Does NOT include fax, phone or video

12

---

---

---

---

---

---

---

---

Slide 13

**INCIDENT REPORTING**

**Information Security Incident** – Any *unauthorized* attempted or successful access, use, disclosure, or destruction of information or interference with system operations.

- ✦ Examples include: viruses, worms, hackers, password sharing, copyright violations, piracy, computer/device theft plus many others

13

---

---

---

---

---

---

---

---

Slide 14

**INCIDENT REPORTING**

- ✦ Every department has a Network Contact (NC) to provide computer/network assistance. Know who your Network Contact is.
- ✦ Know how to contact the HelpDesk if your NC is unavailable, or if you are a student
- ✦ Help safeguard Network Security by reporting suspicious events or conduct to the HelpDesk

14

---

---

---

---

---

---

---

---

Slide 15

**INCIDENT REPORTING**

- ✦ Report to
  - + ITG Help Desk - 4-2222 or helpdesk@ohsu.edu
  - + Integrity Office - 4-8849 or oips@ohsu.edu
  - + Public Safety at 4-4444 or 4-7744 or pubsafe@ohsu.edu
  - + Compliance Hotline - 877-733-8313 (anonymous)
- ✦ The more detail you can provide, the better
- ✦ See more information on reporting security incidents at: [www.ohsu.edu/itg/policies](http://www.ohsu.edu/itg/policies)

15

---

---

---

---

---

---

---

---

Slide 16

**BASIC SECURITY STEPS FOR MY PC/LAPTOP**

- ✦ Use virus protection software & keep it up to date
- ✦ Use a firewall
- ✦ Use an anti-spyware/anti-adware program
- ✦ Keep all applications, including your operating system, patched
- ✦ Don't run programs of unknown origin including e-mail attachments
- ✦ Turn off your computer or disconnect from the network when not in use
- ✦ Use individual logins & strong passwords

16

---

---

---

---

---

---

---

---

Slide 17

**MACINTOSH OS USERS**

- ✦ Upgrade to at least OS9.0 (OSX or higher is better)
- ✦ Visit Apple's security site (OSX) at: <http://www.apple.com/support/security/>
- ✦ Visit Apple's support site (OS9) at: <http://www.info.apple.com/user/macos9/>
- ✦ OSX (like Windows XP SP2) has a definite focus on security features

17

---

---

---

---

---

---

---

---

QUESTIONS/CONTACTS

- \* All approved directives can be found at <http://ozone.ohsu.edu/cc/sec/ispp/>
- \* Questions can be directed to oips@ohsu.edu (OHSU Integrity Office)

18

---

---

---

---

---

---

---

---

# Methods of Communication

## Network Contact E-mail

NCs are added to the NC Mail group and receive network related e-mail messages, notes, and appointments from ITG. The primary responsibility of the NC is to pass along those messages that are pertinent to the department users (e.g. server down times).

NCs will act as the single point of contact for the dissemination of information from the ITG Help desk to their local departments. NCs will receive various types of updates and notifications from ITG regarding the network. It is the NCs responsibility to pass along pertinent information to their end users, and provide explanations where necessary.

## Network Contact Meetings

Network Contact meetings are currently scheduled on the second Thursday of each month from 9:30 -11:00 a.m. in UHS 8B60. Appointments are sent out prior to the meeting. They serve to share need-to-know, general technology and education information and getting to know one another.

### NC Forums

NC-Chat is an informal listserv for NC's to use to discuss pertinent issues to the NC Group. Issues can include discussions about hardware and software not supported by ITG.

To subscribe, send an e-mail to **majordomo@ohsu.edu** and type **subscribe nc-chat** in the message area. It is not necessary to put anything in the subject line.

To unsubscribe, send an e-mail to **majordomo@ohsu.edu** and type **unsubscribe nc-chat userid** (i.e. unsubscribe nc-chat silvac) in the message area. It is not necessary to put anything in the subject line.

## User Groups

**msaccess** is an informal listserv for OHSU users to ask questions and request help.

To subscribe send a e-mail to **majordomo@ohsu.edu** and type **subscribe msaccess** in the message area.

To unsubscribe, send an e-mail to **majordomo@ohsu.edu** and type **unsubscribe msaccess userid** (i.e. unsubscribe msaccess silvac) in the message area. It is not necessary to put anything in the subject line.

# Curriculum

## Employee Training

A variety of employee training courses are available to all employees in the OHSU community. Some courses are available and required for certain groups of employees; others are available for everyone.

Most employee training courses are accessed through OHSU's Employee Learning Portal:  
<http://www.ohsu.edu/learning/>

### TrainingForce

For courses access via TrainingForce, a Quick Reference Guide for using TrainingForce is available at the Learning Portal site: <http://www.ohsu.edu/learning/help.shtml#HowToTF>

To log into the TrainingForce system, use your **Novell login ID and Password**.

In TrainingForce you can:

- View current classes
- Self-register for and/or cancel registrations for classes
- Request courses you don't see
- Have access to your training history

## NC Program Duties and Required Training

### Network Contact 1

The Network Contact 1 (NC 1) assignment will be reserved for NCs with computing knowledge and whose administrator requires that they have the least possible involvement.

Responsibilities include:

- Single Point Of Contact (SPOC) For Submission Of Network Projects And Problems
- Complete And Submit Computing And Networking Forms
- Coordination Between ITG And Their Department For Completion Of Projects
- Other Communications With ITG
- Attend The Monthly NC Meeting(S)
- Responsibilities at this level will not include any troubleshooting of problems, however knowledge of GroupWise, knowledge of web-browsing and understanding of purchasing is required.
- These NC Duties May Fall Within an Existing Position Description as "Other Duties As Assigned".
- Pass Along Relevant (Or Pertinent) Information From ITG To Co-Workers

## Network Contact 2

In addition to the duties of the Network Contact 1, the NC 2 is required to have an intermediate level of computer knowledge to provide basic hardware and software troubleshooting.

- Basic Computer Hardware/Software Troubleshooting
- Basic Knowledge Of All Current Core Applications That Are Used By Your Department
- Completion Of The Training Listed In The Required NC Training Classes Chart
- Assess Departmental Staff Computer Training Needs And Schedule Them For The Appropriate Classes.

Maintenance And Support Of Any Departmental Applications As Outlined In The NC Responsibilities And Procedures Manual

## Network Contact Curriculum

### Class Descriptions: Network Contact Curriculum

For up-to-date Network Contact class schedule and class descriptions go to:  
<http://www.ohsu.edu/etc/classes/schedule.shtml>

<b>NC Classes</b>		
<b>R</b> =Required	<b>E</b> = Equivalent Experience	<b>O</b> = Optional
Class Name	NC 1	NC 2
Getting Started: Level 1	<b>R</b>	<b>R</b>
Advanced Support Techniques: level 2	<b>O</b>	<b>O</b>
Computers & Windows XP Getting Started: Level 1	<b>R or E</b>	<b>R or E</b>
Computers & Windows XP Moving Ahead: Level 2	<b>R or E</b>	<b>R or E</b>
PC Configuration & Trouble-shooting: Level 2	<b>O</b>	<b>R</b>
Network Basics for Macs	<b>O</b>	<b>O</b>
GroupWise – Getting Started :Level 1	<b>R or E</b>	<b>R or E</b>
GroupWise – Message Management: Level 2	<b>R or E</b>	<b>R or E</b>
GroupWise – Calendar Power: Level 2	<b>R or E</b>	<b>R or E</b>
GroupWise – Innovative Tools: Level 2	<b>R or E</b>	<b>R or E</b>

## Suggested End User Curriculum

After assessing departmental staff computer training needs, schedule end users for appropriate classes using the following list.

- Beginning Windows (2 hours)
- Intermediate Windows (4 hours)
- Introduction to GroupWise (4 hours)
- OHSU Services Applications, as needed

## Class Descriptions: End User Curriculum

For up-to-date IT Training class schedule and class descriptions go to:  
<http://www.ohsu.edu/etc/classes/schedule.shtml>

## Computer Proficiency Licenses

The IT Training Center is now a certified testing center for the Microsoft Office Specialist (MOS) exam and the Internet and Core Computing (IC3) certification exam. For more detailed information go to <http://www.ohsu.edu/etc/certification/>

### MOS Certification:

This program is the only comprehensive, performance-based certification program approved by Microsoft to validate desktop computer skills using each of the following Microsoft Office programs:

- Word
- Excel
- PowerPoint
- Access
- The certificate is a valuable credential recognized worldwide as proof that an individual has the desktop computing skills needed to work more productively and efficiently.

### IC3 Certification

This certification includes comprehensive, performance-based certification approved by Microsoft to validate literacy in

- Computing Fundamentals (hardware, software, using an operating system)
- Key Applications (Program, Word Processing and Spreadsheet functions)
- Online Skills (Networks & Internet, E-Mail, Impact of Computing on Society)

# Appendix – Resources

# Computer Skills Checklist

ITG recommends that all OHSU computer users seek to attain a basic level of proficiency in order to make effective use of the information systems on which the university is becoming more and more reliant. Faculty and staff are committed to providing training and assistance so that all users can work at this minimum level of self-sufficiency. Please contact the **Help desk at 494-2222** or the IT Training Web Page <https://trainingforce.ohsu.edu/registration/> for advice on training classes, which will help users acquire any or all of these skills.

All OHSU users should be able to understand and manage these basic computer literacy skills.

## FILE MAINTENANCE

- Open files
- Save files
- Locate files
- Rename files
- Delete files
- Copy or Move Files, including to/from external media
- Use Find, including advanced options
- Save As a new file format, and knowing when and why to use it
- Understand the implications of file extensions and associations

## DIRECTORY MAINTENANCE

- Use directory structures to organize documents
- Create, Rename and Delete folders

## MANAGE DESKTOP

- Manage open windows
- Minimize or maximize, or resize a window
- Understand the concept of active and inactive windows
- Access a specific application when several are open

## WORD PROCESSING

- Page formatting
- Text formatting (font type, size bold, italic, etc)
- Use of Tool bars, spell checking, print preview, search and replace
- Negotiating multiple open word-processing documents
- Setting up preferences and options such as automatic backup, preferred directories, etc.

## CUT, COPY, AND PASTE

- Text and Graphics from one document to another
- Text and Graphics from one application to another

## IMPORTING TEXT FILES

- Know how to import text files with .txt extensions into spreadsheets, databases or word processing documents

## PRINTING

- Shift between local and network printing or between network printers
- Cancel or suspend a print job

## EMAIL

- Compose, address and send messages
- Add, open and save attachments
- Print messages and attachments
- Manage folders
- Create personal address lists
- Archive email
- Change preferences and/or setup

## BASIC NETWORK SKILLS

- Understand Universal Naming Conventions (UNC) and virtual drive letters (i.e. lair1 on 'Home9/910' (H:))
- Browse for things you cannot immediately find

## BASIC HOUSEKEEPING SKILLS

- Determine how much space a file or directory occupies
- Determine available free space on a drive; know what to do if your hard drive is full
- Defragment your disk
- Check for viruses
- Zip/unzip files
- Deleting archived email

## INTERNET/INTRANET (O-ZONE)

- Browse the web
- Read OHSU campus news groups
- View events on the OHSU campus calendar

- Understand the distinction between the OHSU internet and O-Zone (intranet) pages

## NC Web Sites

The following are a list of useful web sites for information gathering and troubleshooting. Please be aware that site addresses change from time to time so these links, current today, may be out of date at some point.

<b>Microsoft</b>	
Microsoft's Home Page	<a href="http://www.microsoft.com/">www.microsoft.com/</a>
Microsoft's Support Page	<a href="http://support.microsoft.com/directory/">support.microsoft.com/directory/</a>
External Microsoft Office Support Pages	<a href="http://www.ohsu.edu/etc/support/index.shtml">www.ohsu.edu/etc/support/index.shtml</a>
<b>ITG Help desk Knowledge Base</b>	Type "helpdesk" on any OHSU web page
MVP (Microsoft Valued Professional) Page – List of all MVPs' web sites – provide support, tips on Microsoft products	<a href="http://www.mvps.org/">www.mvps.org/</a>
Discussion Groups – peer support of Microsoft products; MVPs contribute as well	<a href="http://www.microsoft.com/office/community/en-us/default.aspx?d=1">www.microsoft.com/office/community/en-us/default.aspx?d=1</a>

<b>Novell – Software Publisher of GroupWise and OHSU's network operating system</b>	
Novell's GroupWise Knowledge Base	<a href="http://support.novell.com/search/kb_index.jsp">http://support.novell.com/search/kb_index.jsp</a>
GroupWise Cool Solutions, Tips, feature and downloadable GroupWise manuals and quick reference guides	<a href="http://www.novell.com/cool solutions/gwmag/">www.novell.com/cool solutions/gwmag/</a>
GroupWise Web Access	<a href="http://www.ohsu.edu/gwsecure/">www.ohsu.edu/gwsecure/</a>

<b>General Support</b>	
Apple Support	<a href="http://www.apple.com/support/">www.apple.com/support/</a>
Adobe Support	<a href="http://www.adobe.com/support/main.html">www.adobe.com/support/main.html</a>

<b>OHSU Web Sites</b>	
ITG Home Page	<a href="http://www.ohsu.edu/itg/">www.ohsu.edu/itg/</a>
<b>ITG Computer Access</b>	<a href="http://ozone/itg/cacc/">http://ozone/itg/cacc/</a>
<b>ITG CAPS Web Site</b>	<a href="http://helpdesk/viewindex.aspx?key_id=1376">http://helpdesk/viewindex.aspx?key_id=1376</a>
Employee Learning Portal	<a href="http://www.ohsu.edu/learning/">www.ohsu.edu/learning/</a>
<b>IT Training Home Page</b>	<a href="http://www.ohsu.edu/etc/support/index.shtml">www.ohsu.edu/etc/support/index.shtml</a>
IT Training Support Home Page	<a href="http://www.ohsu.edu/etc/support/index.shtml">www.ohsu.edu/etc/support/index.shtml</a>
IT Training NC Home Page	<a href="http://www.ohsu.edu/etc/nc/index.shtml">www.ohsu.edu/etc/nc/index.shtml</a>
Library Home Page	<a href="http://www.ohsu.edu/library/">www.ohsu.edu/library/</a>
Mac Engineering Page	<a href="http://mac.ohsu.edu/">http://mac.ohsu.edu/</a>
ITG Hardware/Software/Forms	<a href="http://helpdesk/viewindex.aspx?key_id=1376">http://helpdesk/viewindex.aspx?key_id=1376</a>






**(continued)**

### Additional Resources

SIIA (Software & Information Industry Association)	<a href="http://www.siiia.net/piracy/">http://www.siiia.net/piracy/</a>
Business Software Alliance	<a href="http://www.bsa.org/usa/antipiracy/">http://www.bsa.org/usa/antipiracy/</a>

# OHSU Drive Definitions and Usage for PCs

Drives are defined by letters of the alphabet, followed by a colon. Example – A:

Drive	Definition	Comment
A: or B. drives	 <b>Floppy drives for floppy disks</b>	The letters A and B are always reserved for floppy drives.
C: drive	 <b>Computer workstation's primary hard drive</b>	Hard drives (disks) are located inside the computer workstation.
D: – G: drives	 <b>Additional hard disks, CD-Rom drives, Zip or Jazz drives, “Thumb” or portable USB drives</b>	These drives are also physically attached to the computer workstation
<b>OHSU Network Drives</b> 		
<b>H: drive = home server*</b>  <b>*NC can provide specific home server information</b>	 <b>Network drive available to the individual user.</b> Recommended drive for storing files. H-drive backups are performed nightly	You must be logged into the network to access the H-drive.  You may access your H-drive from any OHSU workstation, by logging into the network with your full context name.
<b>I: drive = Share1 Three main areas</b>	<b>Inter-Departmental share area</b> – for collaboration across different departments	<b>All of OHSU can use some portion of this area to share content</b>
	<b>Transfer Holding area</b> (i:\ohsu\transfer) – for inter-departmental <i>temporary holding and delivery</i> of content to other OHSU users. <b>Not a permanent storage area.</b>	<b>CAUTION:</b> Do not <i>store</i> files (especially files with phi content) in the Transfer temporary holding area. <u>Any OHSU user can read, copy, edit, or delete any files in the Transfer area.</u>
	<b>Public area</b> (i:\ohsu\public) – To read and copy OHSU forms and files, mostly from administration departments	Example: HR Personnel Action forms – i:\ohsu\public\hr\PA forms
<b>J: drive</b>	<b>Departmental share area</b> – for content shared with the whole department or part of a department	Only the department can use this area to share content
<b>K: – M drives</b>	Additional network drives a person may use as needed, such as mapping to the location of another application or service.	NCs can provide additional information about mapping drives.
<b>N: – Z: drives</b>	Network drives used by ITG Networks to hold applications, services, and utilities used by OHSU users	Examples: Novell network utilities, site-licensed applications, etc.

# ACCEPTABLE USE OF COMPUTING AND TELECOMMUNICATIONS RESOURCES

## OHSU Policy Manual

### CHAPTER 11 - INFORMATION TECHNOLOGY No. 11-20-010

[http://ozone.ohsu.edu/policy/pac/chapt\\_11/11-20-010.htm](http://ozone.ohsu.edu/policy/pac/chapt_11/11-20-010.htm)

**Effective Date: January 10, 2006**

#### 1. Applicability

This policy applies to all users of University computing, telecommunications and wireless resources, including but not limited to computers, computer systems and networks, portable digital assistants (PDA's), telephones, pagers, cellular phones and two-way radios, whether affiliated with the University or not, and to all uses of those resources, whether on campus or from remote locations. These resources are hereinafter referred to as "computing and telecommunications resources." Additional guidelines may be established by OHSU to apply to specific computers, computer systems, networks or applications.

#### 2. Requirements

##### A. Legal

A user of University computing and telecommunications resources shall comply with all federal, Oregon, and other applicable laws; all generally applicable University rules and policies; and all applicable contracts and licenses. Examples of such laws, rules, policies, contracts, and licenses include, but are not limited to, the laws of libel, privacy, copyright, trademark, and child pornography; the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act, which prohibit "hacking", "cracking", and similar activities; Federal Communication Commission regulations; the University's Code of Conduct; the University's sexual harassment policy; and all applicable software licenses. Users who engage in communications with persons in other states or countries or on other systems or networks should be aware that they may also be subject to the laws of those other states and countries and the rules and policies of those other systems and networks. Users are responsible for ascertaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses.

##### B. Authorized

A user of University computing and telecommunications resources shall use only those resources that they are authorized to use and use them only in the manner and to the extent authorized. Ability to access computing resources does not, by itself, imply authorization to do so. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before accessing any computing resources.

Accounts and passwords may not, under any circumstances, be shared with, or used by, persons other than those to whom they have been assigned by the University.

A user of computing and telecommunications resources shall respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected. The ability to access other persons' accounts does not, by itself, imply authorization to do so.

##### C. Reasonable

A user of computing and telecommunications resources shall respect the finite capacity of those resources (including, for example, bandwidth, disk space and CPU time) and limit use so as not to consume an unreasonable amount of those resources or to interfere unreasonably with the activity of other users.

## **D. Personal**

A user of computing and telecommunications resources shall not use those resources for personal commercial purposes or for personal financial or other gain, except as may be authorized under [Policy No. 10-01-015](#) (Outside Activities/Outside Compensation policy) or institution established news groups.

Incidental personal use of computing and telecommunications resources for other purposes is permitted when the use:

- (1) does not unreasonably consume those resources;
- (2) does not interfere with the performance of the user's job or other University responsibilities;
- (3) does not consume an unreasonable amount of the user's time;
- (4) does not concern subjects inappropriate in a work or study environment (e.g. accessing pornographic web sites);
- (5) is not inconsistent with OHSU's mission of healing, teaching and discovery; and
- (6) is otherwise in compliance with this and other OHSU policies including requirements to reimburse the University where required under [Policy No. 03-25-080\(2\)](#).

Further limits may be imposed upon personal use in accordance with normal supervisory responsibilities.

## **E. E-Mail and OHSU Communications**

E-Mail and calendar systems are designed to facilitate the communication of business ideas and materials pertinent to the operation of the University.

Announcements, bulletins, and documents deemed by management to be of value and interest to the well-being of employees are an integral part of the system. Except as otherwise authorized by collective bargaining agreements or by Employee Communications, all broadcast e-mail (unsolicited messages sent to more than 50 OHSU addresses across departments) must be submitted and approved by Employee Communications and shall be distributed during off-hours by ITG.

Communications over the e-mail system shall be professional and appropriate for the workplace or group setting. E-mail may not be used for personal solicitations or advertising or other activities except through OHSU provided electronic news group systems for those types of activities. Propagation of chain letters is specifically prohibited.

Falsifying e-mail headers (e.g. providing a false sender's address) or routing information so as to obscure the origins of mail or mail routes is forbidden. Altering the content of a message attributed to another is not permitted unless the changes are explicitly noted.

## **F. Representing the University**

A user of computing and telecommunications resources shall not state or imply that they speak on behalf of the University or use University trademarks and logos without authorization to do so. Affiliation with the University does not, by itself, imply authorization to speak on behalf of the University. Authorization to use University trademarks and logos on computing and telecommunications resources may be granted only by University News and Publications. The use of appropriate disclaimers is encouraged.

## **3. Security**

The University employs various measures to protect the security of its computing and telecommunications resources and of their users' accounts. Users should be familiar with OHSU information security practices and engage in applicable "safe" practices, for example, by establishing appropriate access restrictions for their accounts, keeping the network virus-free, safeguarding passwords, ensuring proper physical safeguards, and protecting the confidentiality of electronic protected health information.

#### **4. Expectation of Privacy**

##### **A. General**

University computing and telecommunications resources are not private. For example, communications made by means of these resources are subject to Oregon's Public Records Law to the same extent as they would be if made on paper. The normal operation and maintenance of the University's computing and telecommunications resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for the rendition of service.

##### **B. Reason to Access Activity**

In addition, the University may access or monitor the activity and accounts of individual users of University computing resources, including individual log in sessions and communications, without notice, when:

- (1) The user has voluntarily made them accessible to the public, as by posting to Usenet or a web page;
- (2) It is necessary for OHSU work and business-related reasons (e.g. a person is on vacation or sick leave and access to some files is needed to further institution business);
- (3) It reasonably appears necessary to do so to protect the integrity, confidentiality, availability, or functioning of the University generally or computing and telecommunications resources in particular, or to protect the University from liability;
- (4) There is reasonable cause to believe that the user has violated, or is violating, OHSU policy;
- (5) An account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns; or
- (6) It is otherwise required by law.

Any such access or individual monitoring, other than that specified in 4. A. and B.(1) above, required by law, or necessary to respond to perceived emergency situations, must be authorized in advance by three of the following individuals: Vice president of Human Resources, Legal Counsel, Chief Information Officer, and Information Security Officer. The head of the unit which employs the individual will be notified of such access when appropriate. The University, at its discretion but subject to any applicable laws, may disclose the results of any access or monitoring, including the contents and records of individual communications, to-University personnel or law enforcement agencies and may use those results in appropriate University disciplinary proceedings and/or legal proceedings.

##### **C. Monitoring as a Job or Service Requirement**

The University may also authorize access and monitoring of an employee's or agent's actual communications over its computing and telecommunications resources where customer service is a primary responsibility of an employee's job duties. Such monitoring must be authorized by the Vice President of Human Resources and employees in positions subject to monitoring shall be notified of such activity.

#### **5. Remote Access to OHSU Computing Resources**

A. OHSU employees and students may be authorized secure remote access to information assets owned by or in custody of OHSU. Remote access may be granted by the department director or other appropriate authorizing authority where appropriate to fulfill a person's work or other responsibilities.

B. Remote access for contractors, business partners, referring physicians, other health care providers or other approved users with significant business justification may be approved on a case-by-case basis by an appropriate authorizing authority.

C. Applicants for remote access must submit the OHSU Remote Access form. Information technology support vendors may also be granted remote access for system and application maintenance as negotiated in the support contracts.

D. Noncompliance with the requirements of a remote access authorization or with other provisions of this policy, as determined by the authorizing authority, may result in immediate loss of access privileges and possible corrective or legal action against the violator.

## **6. Enforcement**

Users who violate this policy may be denied access to computing and telecommunications resources and may be subject to other penalties and disciplinary action, both within and outside of the University. Violations will normally be handled through the University procedures applicable to the relevant user. However, the University may temporarily suspend or block access to an account, prior to the initiation or completion of such procedures, when it reasonably appears necessary to do so to protect the integrity, confidentiality, or availability of University or other computing resources, or to protect the University from liability.

---

**Background: formerly Policy No. 08-20-010 (renumbered)**

**Implementation date: June 23, 1998**

**Revision dates: March 1, 2001; August 8, 2001; January 10, 2006**

**Related policies, procedures and forms:**

- **Policy No. 01-05-010, [Confidentiality](#)**
- **Policy No. 01-05-012, [Confidentiality of Health Information](#)**
- **Policy No. 03-25-080, [Use of Institutional Resources](#)**
- **Policy 10-01-015, [Outside Activity/Outside Compensation Policy](#)**
- **Network Services Usage Agreement**
- **OHSU Remote Access Form**
- **Service Observation ([Quality Monitoring](#)) Form**

**Responsible office: Integrity Office**



# Software Management Guide

## *-a guide designed to assist you in effective software management*

### Why worry about software licensing?

In recent years, the issue of software licensing and software piracy has come to the attention of computer users nationwide, often with staggering results. Organizations that saw no problem with copying software for employee use have been hit with stiff fines and other penalties for the mismanagement of the software installed on their workstations. A lax attitude toward software use is often due to the lack of an effective software management policy, employee education, and active support from upper management within the organizational environment. Unfortunately, many people either ignorantly or deliberately jeopardize that growth. Whenever you use a piece of software that is unlicensed, you are depriving the software companies of their earnings. More importantly, you are depriving the creative teams who have developed the software (*e.g., programmers, writers, graphic artists, etc.*) of the compensation for the thousands of hours they have spent working on a particular program. Many computer users have found themselves caught in the piracy trap, unaware that they were doing anything illegal. To avoid such unpleasant surprises, it may be helpful to know the five basic ways a person can pirate software:

1. **Soft Lifting** – Purchasing a single licensed copy of the software and loading it on several machines, contrary to the terms of the license agreement. This includes sharing software with friends and co-workers and installing software on home/laptop computers if not allowed by the license.
2. **Internet** – Uploading (or downloading) commercial software (*i.e., software that is not freeware or public domain*) on an online service or the Internet for anyone to copy or copying commercial software from any of these services.
3. **Hard-disk loading** – Selling computers preloaded with illegal copies of software. If you buy or rent computers with preloaded software, your purchase documentation and contract with the vendor should specify which software is preloaded and that these are legal, licensed copies.
4. **Renting** – Renting software for temporary use, as you would a video. Software rental was made illegal in the United States by the Software Rental Amendments Act of 1990 and in Canada by a 1993 amendment to the Copyright Act.
5. **OEM Piracy/Unbundling** – Some software, known as OEM (original equipment manufacturer) software, is only distributed when sold with specified accompanying hardware. When these programs are copied and sold separately from the hardware, this is a violation of the contract with the publisher. Similarly, the term “unbundling” refers to the act of selling separately software that is legally sold only when bundled with another package. Software programs that are marked “not for resale” are often bundled applications.

As you can see from the various types of piracy described above, it is easy to become an “*accidental pirate*.” This is part of the reason piracy has become so costly to the software industry.

Anyone who purchases a piece of software has the right to load it onto a single computer, and to make one copy for “*backup*” or “*archival purposes*.” That is the **only** copy you are authorized to make according to the terms of the U.S. Copyright Act. Individual software license agreements frequently grant users more rights than they are allowed under the U.S. Copyright Act and may allow for more than a single archival copy, and should be read and understood before using the software. Making additional copies or loading the software onto more than one machine may violate copyright law and is considered piracy.

For more information go to <http://www.siaa.net/piracy/>

## What is the Copyright Law?

# THE U.S. COPYRIGHT ACT

The US Copyright Act, found in Title 17 of the US Code, automatically protects software from the moment of its creation and fixation in tangible form. Except for the rights to (i) copy the software onto a single computer and (ii) make “another copy for archival purposes only,” which are provided in the act (Section 117), any other use without the permission of the copyright owner is prohibited.

The US Copyright Act also gives certain exclusive rights to the copyright owner, namely to “reproduce the copyrighted work” and “to distribute copies...of the copyrighted work” (Section 106). The exclusive right of reproduction includes making copies of computer programs in any format. These formats include CD, magnetic and optical disk, computer memory for personal computers, and networks. The exclusive right of distribution includes any sale, lease, rental, or transfer of such copies. The right of distribution also includes the exclusive right to offer to transfer copies, regardless of whether payment is received. Moreover, it embodies distribution by any means, including electronic distributions via the Internet and other networks.

The US Copyright Act also states that “anyone who violates any of the exclusive rights of the copyright owner...is an infringer of the copyright” (Section 501). This section proceeds to list several penalties for this infringement, including liability for damages suffered by the copyright owner plus any profits of the infringer that are attributable to the copying, or statutory damages of up to US\$150,000 for each work infringed. In addition, the copyright owner can recover attorney's fees from the infringer. The unauthorized copying or distribution of software is a federal crime if done “willfully and for purposes of commercial advantage or private financial gain.” This includes the receipt of anything of value, like bartered software, or willfully making multiple copies with a value of more than \$1000. Criminal penalties include fines of as much as US\$250,000 and jail terms of up to five years.

In simpler terms, if you wish to remain free of legal entanglements, you should be sure you have the legal right to copy or distribute copies of a piece of software before doing so.

## Reasons for Following the Terms of Software Licenses

While computer software is a new form of intellectual property, it is covered under the same provisions of copyright law that protect music, books and film from unauthorized distribution. Like the more traditional media, infringement of copyright law involving computer software carries with it stiff penalties.

All software comes with a license that specifically states the terms and conditions under which the software may be legally used. Licenses vary from program to program, and may authorize as few as one computer or user to use the software, or as many as several hundred network users to share the application through the system. It is important to read and understand the license agreement accompanying the program to ensure that you have sufficient legal copies of the software for your department's needs. Users of software programs need to have a specific contact within their department for their software licensing questions. Appointment of a departmental software manager should be made known to all departmental employees so that specific questions can be asked of the software license in question.

The most fundamental aspect of a successful software policy, outside of the policy itself, is the actual software audit. If a software audit determines that your department is using unauthorized (*i.e.*, *pirated*) copies of software, **OHSU** (not just your department) may face not only a civil suit for damages and any profits attributable to the pirated software, but corporate officers and individual employees may be charged with criminal liability as well. This may also include fines and jail terms. Taking steps to prevent the use of illegal software and ensure compliance with copyright law can save your organization the expense and embarrassment of this kind of legal action.

### Risks of Illegal Software:

- Fines of up to \$150,000 per infringed title.
- Lack of product support
- Blemished reputation – “Hey, you were the one's busted”
- Possible criminal charges against directors/managers

- No product warranties, possible virus infection

# OHSU's Software Copyright Law Technical Directive

## *OHSU's Technical Directive*

### Six-Point Program for Ensuring Software Compliance

This six-point program outlines a number of areas that must be integrated to provide a comprehensive approach to software management within the department. More detailed information follows.

1. Appoint a departmental software manager.
2. Establish procedures for registering, storing, and utilizing software.
3. Establish and maintain a software log.
4. Conduct periodic audits.
5. Establish an employee education program.
6. Maintain a library of software licenses and registration materials.

#### 1. APPOINT A DEPARTMENTAL SOFTWARE MANAGER

The manager is responsible for maintenance of detailed records and supervision of compliance. To ensure a comprehensive, uniformly administered program, employees should have access to a single individual knowledgeable about all aspects of OHSU's software policy. In addition to effective coordination, assigning a person to this role sends a strong signal about the department's commitment to software license compliance to its employees and vendors.

#### 2. ESTABLISH PROCEDURES FOR REGISTERING, STORING, AND UTILIZING SOFTWARE

- a. **Registration.** The software manager should complete registration cards for all software as it is purchased and delivered, or in the case of online software purchases, the software manager should complete the online registration form at the software publisher's website. Promptly completing this process ensures that the department will receive product support and timely product announcements. A Software Log (*see Appendix*) may prove helpful in tracking software acquisitions and registration. **Exception:** Licenses for software purchased OHSU enterprise-wide; e.g., Microsoft Office, GroupWise, SMS are managed through ITG. OHSU ITG maintains a complete list of this software.
- b. **Storage and Security.** After installing the program, the software manager should keep the original software in a separate, secured storage area. By ensuring secure storage, the risk of software theft and unauthorized duplication of software is minimized. Original software should be stored so that they are not subject to damage by environmental factors such as heat, fire, and water.
- c. **Documentation.** Original manuals, tutorials and other user-oriented documentation (if part of the software package) should reside with the software user. If you work in a network environment, you may opt not to distribute a manual to each user, but rather keep manuals in one central location.
- d. **Home Computers and/or Laptops.** If your employees are like most, it is not unusual for them to take work home or bring personal software to the office. This is another area of potential risk. Generally, employees should not be permitted to bring software from home and load it on department computers because of the risk this poses from viruses unwittingly brought in on the employee's software. A department's computers are important assets and risks to assets should be minimized. To ensure that all software used at OHSU is both legal and virus-free, software should be purchased and installed through OHSU's established software acquisition process only.

### 3. ESTABLISH AND MAINTAIN A SOFTWARE LOG

The software manager should maintain a log of all software purchased by the department (*see Appendix*). The software log should note the location of each software package and the Term ID of the computer on which the software is installed. After ensuring that all software has been legally purchased, the audit results can serve as the basis for the software log. The software manager then can update the log database with each new software acquisition. The log should contain the following:

- a. The product name and publisher (vendor) of the software acquisition, and software serial number (if appropriate).
- b. The purchase date of the software.
- c. The name of the authorized user.
- d. The Term ID on which each copy of software is installed.
- e. The existence, location and number of original CDs.

The software manager should also maintain copies of the original license agreement, completed registration cards, and any other documents showing legitimate acquisition of software to have available for future reference. These should be filed with the purchasing documentation.

### 4. CONDUCT PERIODIC AUDITS

An audit of your software resources will provide several benefits to your department. First and foremost, the audit allows you to determine compliance with the various aspects of OHSU's software technical directive [reference to URL]. To be comprehensive, it should include, but not be limited to a review of the following:

- a. The software log and license agreements
- b. The department's software budget
- c. The actual software found residing on the department's computers
- d. The software purchase records

After the audit, remove or purchase (may depend on the department's software budget) any pirated software found on the computers.

### 5. ESTABLISH AN EMPLOYEE EDUCATION PROGRAM

To ensure that your software compliance program is ultimately successful; it should be supported by a department-wide education program. The educational program should have the following components:

- a. Explain the software code of ethics and OHSU's Software Copyright Law Technical Directive.
- b. Enlighten employees about software piracy and why it is a problem.
- c. Explain the hidden costs of illegal software, such as the prospect for fines and possible sanctions against OHSU and/or the employee.

### 6. MAINTAIN A LIBRARY OF SOFTWARE LICENSES

The software manager should not only become familiar with the license agreements of the software products used by the department, but should also be responsible for maintaining a library of product licenses. Departmental employees should be provided with copies of each applicable license agreement, or have access to them.

