WSE IT Policies and Guidelines

Whiting School of Engineering IT
JOHNS HOPKINS UNIVERSITY| WSEHELP@JHU.EDU

Table of Contents

Document History

REVISION	CHANGE
2013.02.12	First circulated draft
2013.02.15	Revised illustration; edit to enforcement section to clarify source
2013.02.26	Added information about superuser and service accounts
2013.03.01	Added reference to student computing policy (resnet); added web project manager hire
2013.03.13	Cellular Phone / Data Policy Added
2013.04.04	Revised "Relationship" section to clarify role of WSE IT
2013.04.15	New introduction, revised relationship language defined commodity services, update for
2013.04.16	Revised Security of IT Resources to clarify options
2013.04.19	Added section on purchasing computers on sponsored projects
2013.04.29	Revised wording to clarify application of policy to non-WSE-IT groups within WSE in introduction and in Relationship… section
2013.05.10	Ernie are not good at grammar – Noah Cowan helped out
2013.06.01	Approved version
2013.10.25	Added section about lab management, added Rustam to staff list
2014.12.22	Updated staff area
2015.11.30	Updated staff area
2016.05.02	Refreshed definition of research computing; cleaned up references to IT@JH; removed obsolete network refactoring diagrams; changed some future-tense specifications to present tense (eg: physical security section)
2016.10.05	Changed in-semester lab software update language to be more realistic about scheduling downtime. Linked to KITCATS lab policy as reference for users of their labs.
2016.10.05	Removed staff list, changed to be information about staffing policies

Overview

Introduction

This document is intended to provide guidelines for the appropriate use of Information Technology within the Whiting School of Engineering. The purposes it hopes to serve include:

- To specify the occasions when IT policy as created by Hopkins Central IT needs to be amended to meet the requirements of the Whiting School
- To provide guidelines for Whiting IT to answer routine questions consistently
- To record answers to unusual questions (for example, for response to audit, or anticipating disaster recovery situations)

Policies here are NOT to be considered as one size fits all. Whiting IT recognizes the dynamic nature of IT in our environment and uses these policies as a starting place for discussion, not as the answer for all situations. They provide guidance for how WSE IT aims to provide IT services, and set expectations for public-facing systems that are not under some other IT group's management. Systems that are the responsibility of another IT group can be managed to that group's standards as long as security requirements are being met.

Definitions

The following definitions apply to IT use inside WSE for the purpose of this document:

- Operational / productivity computing. This is where users are using IT resources to run the operations of the school. Included here is IT used for budgeting and planning, maintaining the records of the school, and IT used to support the marketing efforts of the school. Most of the controls in this document will relate to this IT function.
- Research computing. It is not the intention of WSE IT to be deeply involved in the day to day aspects of research computing except where they can provide supporting infrastructure services and relieve researchers of this burden. To ensure proper security and isolation from other IT resources WSE IT will set policies for the external, public facing aspects of research IT systems and periodically audit those public facing systems.
- Instructional computing. This includes computer labs and student computing. Instructional computing is largely being managed by KSAS' KITCATS group. Because of this, at this time instructional computing is mostly outside the scope of this document. Computing labs operated by departments or research centers used for instruction are expected to have defined boundaries (similar to research computing) so they can be as isolated as possible without affecting their instructional mission.

- Commodity services / supporting infrastructure. These are those services that must be in place for all IT projects to function, where their unique operation for some department or research group would add no additional value. Examples of this would often include DNS, DHCP, and email, and might also extend to basic file and print services, web server services (blogs, wikis, application servers), and license server services.

Relationship between WSE, WSE IT, and other IT groups within WSE

WSE IT is not intended to replace other IT resources currently utilized around WSE. If there is no in-place IT support unit, WSE IT will provide direct user and system support using the guidelines in this document, but where other resources are meeting the needs of their clients WSE wants to continue to utilize and support established teams and processes. To restate, WSE IT is one of several options for direct desktop support, but departments are not required to use our support.

For all affiliates of the Whiting School, no matter where they might obtain desktop support, WSE IT's primary mission is to coordinate IT activities and policies within the school. It looks to ensure that IT resources are deployed in a consistent, well-documented, secure, cost-effective manner across departments, centers, and administrative units. In particular, its aim is to define and standardize the commodity services of the infrastructure to ensure there is a solid, effective underlying layer for the unique IT requirements throughout the school.

WSE IT aims to be a repository of IT best practices and policies, and to advocate for appropriate IT resources for the WSE community with the WSE deans, with IT@JH, and with vendors. It also will be responsible for developing and maintaining relationships with IT communities such as Educause, and to gain understanding of the IT landscape through networking with and from benchmarking against peer institutions.

Conflicts with other policies

This document is intended to supplement the policies and procedures documented Hopkins-wide by IT@JH. IT@JH's IT policy documents can be found at http://www.it.johnshopkins.edu/policies/. Where there is a gap, the IT@JH policy is in effect. Where there is a conflict, the WSE IT policy is in effect. To be explicit, this document is intended to supplement the IT@JH Acceptable Use Policy, Log Management Guidance, Removal of Data from Hard Drives and Electronic Media Standards, Guidelines, and Procedures, Project Application Service Systems Support Documentation, Vendor Application Host Security Checklist, and Vendor Remote Access Contract.

Enforcement

The University Acceptable Use Policy takes enforcement of IT policy seriously. To quote the IT@JH AUP: "The failure by personnel to comply with these policies may result in the loss of access to some or all of the IT resources of the University. Additionally, violators of these and other University IT policies may be subject to criminal and/or civil penalties and to disciplinary action, up to and including termination."

Sponsorship and Review

This document is maintained by the WSE IT staff, approved by the WSE IT Director and the Senior Associate Dean for Finance and Administration, and ratified by the WSE IT Faculty Advisory Group. It will be reviewed at least every two years.

WSE IT Faculty Advisory Group

The WSE IT Faculty Advisory Group advises the WSE IT Director and the Senior Associate Dean for Finance and Administration on issues of IT strategy. It is composed of no more than eight faculty members from the college and meets quarterly. The Group discusses IT concerns of long-term consequence that require substantial investment in money or effort.

The IT Faculty Advisory Group was formed to focus on big-picture concerns. Feedback on daily operations or any other topic is welcomed by the IT staff at wsehelp@jhu.edu or by contacting the Director.

Acceptable Use of IT Resources and Security

Whiting School Addendum to the IT@JH Acceptable Use Policy

WSE IT endorses the acceptable use policy as documented on the IT@JH website, and requires acknowledgement of that policy for access to University IT resources. It is the goal of Whiting IT to have all user systems meet the security and management standards set by the IT@JH policy (for example, to use enterprise authentication unless absolutely necessary to aid in user provisioning / deprovisioning) except when absolutely necessary.

Security of IT Resources

The Whiting School's worldwide reputation for cutting-edge research requires intensive use of IT. It is recognized that the requirements for IT resources in research are often incompatible with normal IT operating standards for areas such as patch management, antivirus use, and account security. To provide the flexibility required for research while preserving the confidentiality, integrity, and availability

of the larger community's IT resources, research IT resources will be reviewed for security issues and if issues are found a remediation plan will be developed. In some cases the researchers may prefer "hardening" their systems, but to minimize impact to the research program it will often be preferable to isolate the systems from both the public Internet and from the publically- and privately-addressed general use JH internal networks. With isolation, security-related configuration and management of research IT resources can remain entirely at the discretion of the researcher. Systems that bridge the boundary or are public facing (even if only to the JHU networks) will need review for proper security and management practices, but those inside will not.

Lab equipment often requires security settings or patch management exceptions that would be unacceptable in the general population. Lab equipment requiring these exceptions (for example, running older operating systems no longer supported by security patches) need to be isolated from the public internet and from the general-use internal Hopkins network.

Physical Security of IT Resources

For WSE IT datacenters, access is controlled physically with a swipe card or smart key and approval for access must come from the IT Director. The IT Director will review access lists annually. WSE IT network equipment physical security will be maintained in the same way. Most network closets in WSE are administered by IT@JH. For WSE data centers:

- The most sensitive equipment (primary SAN, virtual machine hosts) is installed in the Mt. Washington datacenter and has all of the access controls of that facility
- Second-level equipment (sensitive but not mission critical) is consolidated in Garland 15, which is only accessible by Whiting IT staff and escorted visitors
- Third-level equipment (primarily non-sensitive research computing) is consolidated in Garland 6, which can be accessed directly by graduate students and other researchers after being granted swipe access

Determinations on the sensitivity of data on research machines are the responsibility of the researchers. WSE IT can consult on data protection, but cannot judge the sensitivity of researcher data.

Electronic Information Backup, Recovery, and Disposal

Users are encouraged to keep as much data as possible on servers maintained by their IT support team. Servers will generally provide the highest level of protection against loss due to hardware failure.

WSE IT has options available for backup of server and laptop/desktop machines.

As with the security requirements of protecting research data, WSE IT cannot make determinations of the backup requirements of research data. Some data can be easily recreated, and some will be unique and irreplaceable. Researchers should work with WSE IT to ensure their data is protected appropriately. IT@JH policy has documentation for the transmission, handling, and backup of data. It also documents the appropriate steps required to dispose of equipment that has housed sensitive data.

Logging, Monitoring, and Scanning

As a part of maintaining the IT infrastructure, WSE IT collects a variety of information about the activity on its systems. This information is considered to be confidential and is only used to ensure the confidentiality, integrity, and availability of JHU's IT infrastructure.

A centralized log monitoring system is being developed to ensure that log information can be kept consistently and can be correlated across components of the infrastructure. Critical infrastructure points (boundaries between public and private networks, VPN devices, and access gateways) will be required to ship a copy of their logs off to this log monitoring system.

Subnets are monitored for new IP address activity, but as admission control is at this point inconsistently applied that information is currently of limited use. Eventually this information will also be copied to the log monitoring system.

Machines on WSE subnets that are on the WIN domain have KACE agents installed automatically to monitor their hardware and software configurations. Changes are logged automatically. Using data collected by the KACE agent, reports are generated for patch and antivirus / malware compliance.

When necessary, the free text field in the KACE record is the place where notes about systems will be kept and tracked.

The KACE agent will also be used to track license compliance when some other mechanism (such as a Flex server) is not already provided.

Systems Containing Sensitive Information

If a system is identified as containing sensitive information and is outside a protected research environment it will be expected to meet the following standards. Even when in a protected research environment, researchers are encouraged to use as many of these controls as practical:

- Configuration integrity checks

- Vulnerability monitoring
- Performance monitoring with alert triggers
- Retention of security logs for at least 90 days, containing
    - Successful and unsuccessful access attempts
    - Configuration changes
    - Deactivation of security tools
    - Intrusion detection
    - Database activity monitoring

Public and Private Networks

Private network addressing is often used to hide machines from easy access on the public Internet. Often, users or administrators will assume that because a machine is privately addressed it is unreachable from attackers and that care does not need to be taken in configuration or patching. Because of the network's design at JHU this is a bad assumption as public and private machines are often intermixed, and a compromised public machine will often act as an easy gateway to the private network.

This leads to the following configuration requirements for systems at WSE not otherwise covered by the research configuration described above.

- Whenever possible, privately and publically addressed networks should not share the same network segments.
- The boundaries between public and private networks should be guarded by a system (such as a firewall) that can audit the connections traversing the boundary.
- Whenever possible, systems on private networks should be maintained as carefully as those on public networks. This means disabling unused system services, keeping system patches up to date, and running antivirus / antimalware software.

Incident Handling

IT@JH has their own incident handling group reachable at incident@jhu.edu. They notify WSE IT when incidents occur inside Whiting but often there is a delay, so for this reason we appreciate a cc to our support box at wsehelp@jhu.edu. If your incident is not receiving prompt attention or potentially has significant impact to the school or the University, the IT Director and the Senior Associate Dean for Finance and Administration should also be notified.

Antivirus / Antimalware

All customers running Windows must have antivirus / antimalware software installed if they are going to connect to the WSE network. Macintosh users are

strongly suggested to run antivirus / antimalware software. This includes both desktops and servers.

The WSE standard for antivirus software for Hopkins owned machines is Microsoft System Center Endpoint Protection for both Macintosh and PC. It can be downloaded for free from IT@JH at

http://www.it.johnshopkins.edu/antivirus/

Computers not owned by Hopkins must run a similar, frequently updated, well-regarded AV software package.

Miscellaneous Concerns

Change Requests

Functional and technical owners who need to apply changes to their systems that will have broad community effect are required to put that request in in writing to the IT Director for approval, scheduling, and possible community notification. This should include all changes significant enough to make use of the maintenance window.

Software Development

Managing software development for research computing is the responsibility of the researchers. WSE IT will provide one or more source code control tools to facilitate management of code if researchers would like to use such a service.

For WSE IT projects, the SDLC is co-managed by a project sponsor from the line of business being supported by the development and a WSE IT representative. The WSE IT rep will document communications, requirements, project phases, and code changes in the WSE IT shared documentation database, while the project sponsor will develop the business requirements. The IT rep and the project sponsor will together be responsible for developing and implementing test plans and change control as appropriate for the sensitivity of the project.

Vendor Access

Except in extraordinary cases, direct local or remote access to systems will not be given to vendors. If at all possible, when working with a vendor to resolve a problem people should use a recorded screen sharing session to work through the issue so there is a record of the interaction. Exceptions will be reviewed by the IT Director.

If direct, unmonitored vendor access is required then it should be done in accordance with IT@JH's Vendor Access Process. In particular, vendors should have individual named accounts to provide direct accountability for changes.

Superuser Access / Service Accounts

Whenever possible, all system access will be given to individually named accounts. For superuser or root tasks, an individually named admin account will be used (for Windows) or the sudo command will be used to escalate priviliges (for Unix). Direct Administrator or root login is discouraged as it obscures the audit trail for system tasks.

Similarly, limited-privilege (for example, without interactive login) service accounts should be used whenever possible to reduce the effect of a compromised password.

Maintenance Window

The standard WSE IT maintenance window is Friday morning between midnight and 6 AM. IT tasks that may interfere with the normal operations of systems should all occur during this time.

Community Notification

WSE IT recognizes that users may become numb to communications if they are overused. Email notices to the community will therefore be limited only to critical issues that may affect many users, but where that effect can't be isolated to individuals. These emails are sent at the discretion of the WSE IT Director, in consultation with the Director of Marketing Communications.

Guidance for Purchasing Computers on Sponsored Projects

According to Holly Benze (hab@jhu.edu), Director of Research Projects Administration, more and more federal agencies are questioning and disallowing the purchasing of computers and related devices on sponsored projects. She has available a document which offers guidance on when the purchasing of computers for your project can be justified. It also contains policies from several of the federal agencies.

If you have any questions, please call or email your RPA contact.

Purchasing of Retired or Surplus Equipment

When computer equipment is retired or deemed surplus and is no longer needed by WSE it may be purchased by employees. Equipment is designated as surplus by the person authorizing the replacement purchase (if any). The supervisor of the

purchasing employee makes approval for the purchase. Pricing will be set on the basis of a five-year replacement cycle, so if a computer were four years old the sale price would be one-fifth of the original purchase price.

Cell Phones and Mobile Data

Johns Hopkins Accounts Payable department sets policy for cell phones and their voice/data plans. The policy is maintained at https://apps.finance.jhu.edu/policyapp/displayGuideContents.do?guideId=CT

Computer Lab Operations

Overview

Most computer labs on campus are operated by KITCATS. Software installed in their labs is covered under their request policy as described at http://classrooms.johnshopkins.edu/softwarerequest.html. Note that they have different timelines for software requests than WSE IT describes below.

WSE IT can help operate departmental and center computer labs. We have an infrastructure ready to facilitate the imaging and maintenance of the software on lab PCs. Maintaining an up-to-date and stable lab image is a challenging project, however, so we ask for your consideration of the following issues if you wish us to provide this service. In particular, as many labs need to be completed at the same time (at the start of classes) we have long lead times to ensure all work can be done by your deadline.

Deadlines

- For a new project, or for major changes to an existing lab, WSE IT needs notice five weeks in advance of when the work needs to be completed.
- In all cases, WSE IT needs all software binaries and licenses delivered to us three weeks in advance of when the work needs to be completed. Software licenses can take a long time to procure, so please monitor expiration dates carefully.
- WSE IT needs someone to be available to check the software is functioning correctly one week in advance of the deadline for the software to be available. (While we can ensure regular productivity software like Microsoft Word and web browsers function correctly, we don't know how to rigorously test the functions of specialized software.)
- In-semester changes are difficult because updates can only be made when adequate lab downtime is available. Changes will be made as promptly as possible, but often cannot be scheduled until semester breaks. Also, someone will need to be available to check the lab image to ensure the new

software functions correctly and that older software wasn't affected by the change.

Considerations

- The computers within the lab should be all the same model and have close to the same configuration. This lets us build a common image for all the machines.
- We can limit logins to the machines through membership in a group in the campus' Active Directory server. WSE IT will work with departments to configure this, but group membership will be administered by departmental staff.
- WSE IT can provide auditing of printer usage, but for pay-for-print services we will have to work with the campus' libraries who run pay-for-print for the campus.
- No user data should be saved on computer lab computers – it should all be saved to USB drive or a network share. The local drives are subject to being erased as a part of the maintenance to keep the computers secure and functional.
- Whenever possible, site- or network-based licenses should be used in labs. Software that is individually keyed to a specific machine makes maintaining a single machine image impractical, and adds greatly to the time required to prepare a lab. WSE IT is happy to take over the operation of network license servers.

Contacts and Escalations

General IT Support

IT support questions should be addressed to the WSE IT help desk system, reachable by email at wsehelp@jhu.edu. Using this address is encouraged as messages to it are tracked in a database and won't get lost in any one person's inbox. Users can expect a response within one business day. Hours of operation are 8AM to 6PM Monday to Friday.

Student Residential Computing Information and Policy

Information about student computing in residence halls is maintained on IT@JH's ResNet site at http://www.it.johnshopkins.edu/services/network/resnet/. It defines permissible activities and devices for the Hopkins networks for students on the residential networks. The residential network policy is not the same as the academic or lab policy.

WSE IT Staffing Policy

As a condition of employment, all WSE IT staff are required to sign an agreement stating that they will not disclose any data they might encounter as a part of their duties unless failure to disclose that data might be a violation of law.

Any questions about services offered or concerns about services provided can be addressed to the Director.