

Computer Abuse Investigation Checklist Guideline
For
Department Systems Administrators

***Do Not Begin Investigation without first contacting
Human Resource Services
335-4521***

EXCEPTION & IMPORTANT NOTICE:

Suspected Child Pornography, Terrorist Activity or Gambling abuse should be reported immediately to Human Resource Services and the WSU Police. Any investigative activity by department should cease.

Preliminary Steps

- Allegation is reported to dean/director or designee.
- The dean/director or designee contacts Human Resource Services (HRS).
- HRS and the department determine if the department systems administrators should conduct investigation and obtain approvals under applicable policies.
- HRS and the department determine if the Internal Auditor should be contacted.
 - HRS determines if IT security representatives should be involved in investigation – if yes, HRS will contact IT security representative.
 - HRS and the department establish grounds for investigation.
- HRS and the department develop investigation plan that defines the scope of the investigation including the co-investigator.
- Identify primary investigator and co-investigator. Both must be present when accessing computer

Computer Investigation

Recommended steps to follow:

- Secure hardware with co-investigator
- Specify hardware to be reviewed
- Preserve date and time stamps
- Document hardware configuration of system
- Move to secure location
- Mathematically authenticate data on all storage devices (CRC)
- Make a "Bit Stream Backup" of HD
- Make image of partitions is applicable
- Burn CDs of images
- Attach HD as read only drive in second machineBit stream copy of HD contents to partition in second Machine

Examination

Note: Depending on specifics of allegations processes may differ between cases.

Survey of representative sample on system. Document steps and print all results that show misconduct.

Recommended steps:

Examine Web Browsers

Search target: initially, subject lines/addresses to determined non-deminimus, non-work related web activity

- Cookies (both Netscape and IE)
- Cache
- Bookmarks
- History
- Windows Swap File
- Web mail

Examine E-mail

Search target: non-deminimus non-work related E-mail on various clients.

NOTE: IT administer email serves only

- Folder Indexes
- Attachments
- Message Content

Examine UseNet

Search target: non-deminimus non-work related USENET activity.

- Check for Usenet Client
- Check for Usenet Activity

Additional Review Options

- Search for other network apps (search target: i.e. irc etc.)
- Examine directories for installed programs/executables (search target: Pirated code)
- Examine win registry for left over entries from program un-installs (search target: removed code)
- Examine directories for data files (search target: non deminimus non work related data)
- Examine OS logs. (Search target: suspicious log activity)
- Evaluate Unallocated Space (search target: Erased Files)

SUMMARY REPORT

- Document results and findings.
- Complete summary report. (HRS has sample report available)
- Report findings to dean/director or designee and HRS.
- Forward copies of software used to HRS.

APPLICABLE LAWS AND POLICIES INCLUDE: WSU Executive Policy #4 Electronic Publishing and Appropriate Use Policy, WAC 504-25-085, Computer Abuse; RCW 42.52.160, Use of Persons, Money, or Property for Personal Gain; BPPM 20.35, Use of University Property; BPPM 20.37, Personal Use of University Resources; BPPM 35.30, Duplicating and Using Software.