MIDTERM

CYSE 407

Abstract

I have been hired to create and run a brand-new digital forensics lab for a mid-sized police department. Enclosed is my plan for the lab for the next 3 years.

Bryant Watkins

Accreditation Plan

Scope

The objective of the standard is to successfully uphold the validity and integrity of all work to be done by technicians. ISO/IEC 17025 is the international standard for testing and calibration laboratories (iso.org). ISO/IEC 17025 is a standard that allows labs to showcase their competent operations and ability to generate valid results. Achieving such a standard promotes confidence in one's work across global and national fields. Achieving ISO/IEC 17025 accreditation entails having the laboratory's quality management system and technical competence evaluated thoroughly by a third-party. Audits conducted on a regular basis is expected in order to maintain accreditation. Such accreditation is only granted by an authorized accreditation body. Once Accreditation has been established – that means that the laboratory has officially met the specific management and technical requirements of ISO/IEC 17025 and therefore is deemed "technically competent to produce calibration and testing results" (Campbell Scientific).

Reference

ISO/IEC 17025:2017

Terms

Audit - An official inspection of an individual's or organization's accounts, typically by an independent body. (Oxford Languages)

Personnel - The people who work for an organization (Oxford Learners)

Log – Documentation that is a record of all arrivals and departures as well as identifying information

Sanitation - The process of keeping places free from dirt, infection, disease, etc. (Britannica Dictionary)

Maintenance - The process of maintaining or preserving someone or something, or the state of being maintained (Oxford Languages)

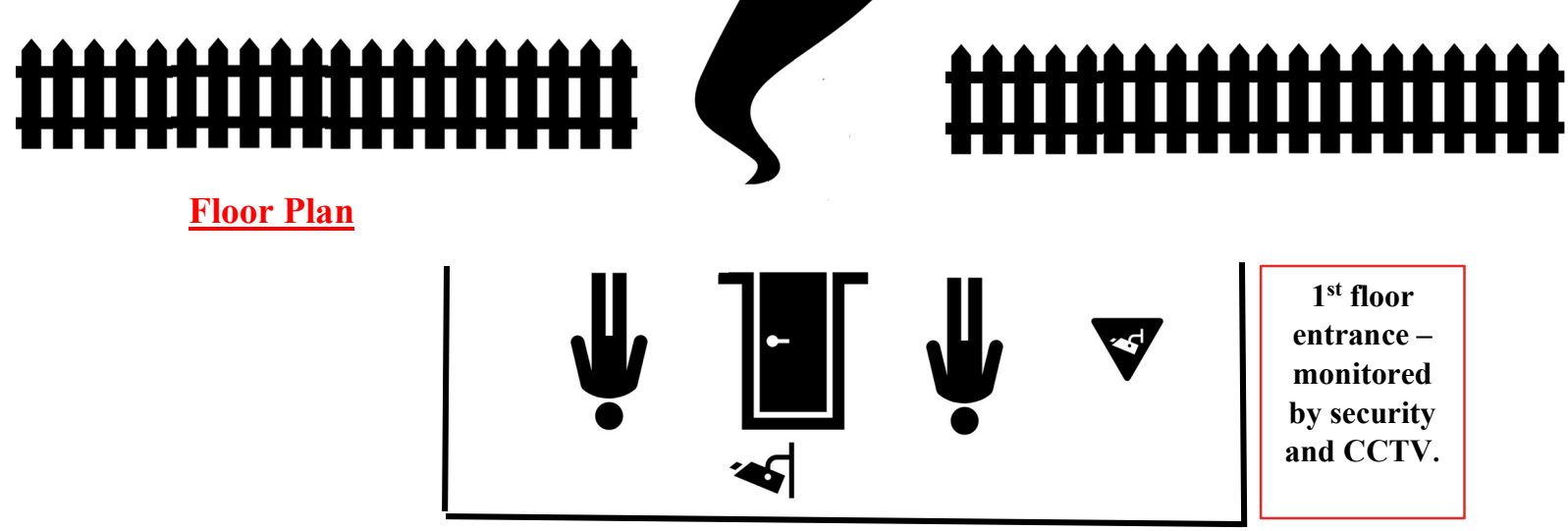
CCTV – Stands for Closed Circuit Television and pertains specifically to surveillance security cameras

SATA – Serial AT Attachment

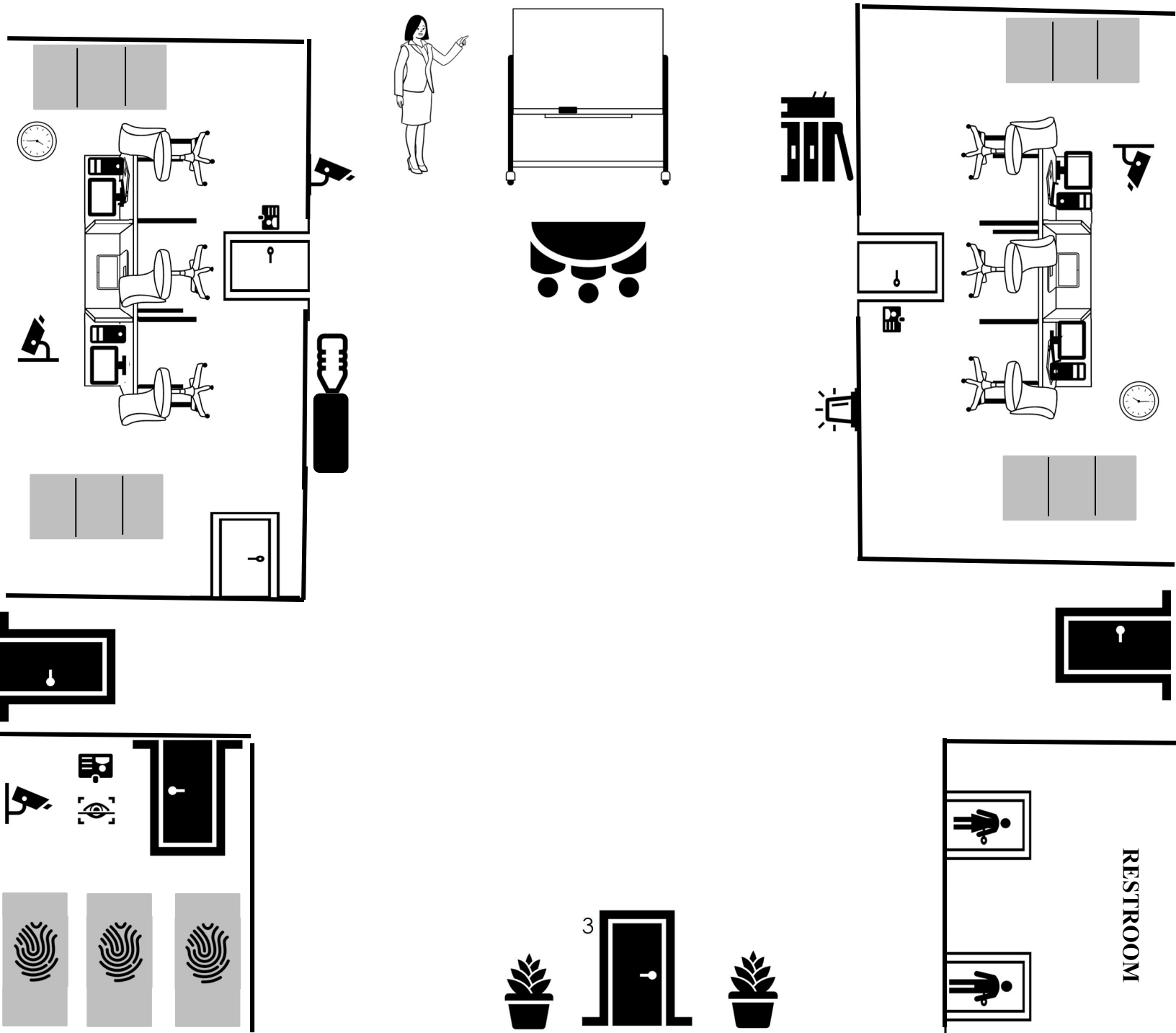
SCSI – Small Computer System Interface

Shall - Expressing a strong assertion or intention (Oxford Languages)

Floor Plan



1st floor entrance – monitored by security and CCTV.



Inventory

- A digital camera for still and motion recording
- Antistatic bags
- External CD/DVD drive(s)
- Ribbon cables for floppy disks
- Extra USB 3.0 cables
- SATA cards/associated cables
- Extra SCSI cards (ultrawide)
- Graphics cards, Peripheral Component Interconnect (PCI) and Accelerated Graphics Port (AGP)
- FireWire & USB adapters
- Variety of hard & USB drives
- Computer hand tools - Phillips and flathead screwdrivers, socket wrench, miscellaneous vendor-specific tools, small flashlight, and antistatic wrist straps
- Microsoft Office (including current and older versions)
- Hexadecimal editor - WinHex
- Programming language - Python
- Specialized image viewers - Quick View, ACDSee, ThumbsPlus, and IrfanView
- Accounting applications – QuickBooks
- Multiple surveillance cameras to observe traffic in all areas
- Security personnel at entrance
- Visitor logs (Physical) for entrance and evidence storage room (Biometric)
- Badge and Retinal scanners to access evidence room

- Fingerprint scanner for access to materials within evidence lockers
- Siren/alarm for unauthorized or forced access to facility or evidence room/locker
- Three evidence lockers (can store up to 20 cases)
- Multiple analysis computers/laptops
- Main office printer/scanner/fax
- Specialized trash bins – one for insignificant items and one for sensitive materials that need to be properly destroyed/disposed
- Chairs/Tables
- Encryption
- Adequate temperature/humidity control system
- Monitors
- Antivirus/Antimalware software – McAfee
- Microsoft Windows 10, 8.0 and 8.1, 7, Vista, XP, 2000, NT 4.0, NT 3.5, 9x, 3.11, and DOS 6.22
- Mac OSs include - macOS, Mac OS X, 9.x, and 8
- Linux OSs include - Linux Mint, DeftZ, Fedora, Ubuntu, Slackware, and Debian

Lab Maintenance Plan

This forensics lab shall be maintained 24/7 to ensure the safety and integrity of all evidence, materials, and lab personnel. Damage(s) that may occur to any facility assets or infrastructure will result in immediate repairs and/or replacement. Security staff and personnel will be sure to escort cleaning crews into the facility, as well as monitor them as they work. Out of abundance of caution - antistatic pads will always be placed around

electronic workbenches and workstations. Floors and carpets will be cleaned daily to assist minimizing dust that may accumulate and cause static electricity.

The visitor log at the entrance shall entail - the visitor's name, date/time of arrival and departure, reason for visit, name of employer as well as name of the lab staff member welcoming the visitor. Anybody who is not assigned to the lab will be considered a visitor for security purposes, including – sanitation personnel, facility maintenance personnel, friends, and family. All visitors will then get escorted by an appropriate security official for the duration of their visit to the lab to ensure that they do not tamper with an investigation or evidence – whether it be accidental or intentional. A visitor badge shall be issued and mandated to be visible at all times to let all investigators know that a visitor is present. Alarm systems and on-site security personnel will also be used after business hours to monitor the lab facility.

Staffing and Job Descriptions

"The ANAB states that each lab should have specific objectives that a parent organization and the lab's director or manager have determined" (Bill Nelson, et al 2018). The primary positions found within the lab environment are lab manager and lab technicians. There are other miscellaneous positions such as that of the security staff, sanitation personnel, and maintenance teams/contractors. Such miscellaneous positions are typically handled through contract agreement(s).

The most critical position is that of ***lab manager***. The lab manager position maintains more responsibility than any other position at the lab. The lab manager is expected to assemble processes for managing cases as well as review them on a regular basis. The general management tasks include the following: pushing for group consensus

in decision making, overseeing fiscal responsibility for lab requirements, and enforcing ethical standards or principles among lab facility personnel. The lab manager will also plan updates for the lab - such as new software/hardware purchases.

The lab manager is expected to establish as well as promotes quality assurance processes for the lab's staff to adhere to – i.e. outlining what to do when cases arrive, logging evidence, specifying who has access to the lab, and creating guidelines for filing reports adequately. The lab manager will also be responsible for setting reasonable production schedules for processing work, doing so will help to ensure lab efficiency. The lab manager will create and monitor lab facility policies to ensure that a secure and safe workplace is afforded for all staff and evidence accordingly. The most critical responsibility of the lab manager above all else is the accounting for all activities the lab's staff conducts to complete its work. Monitoring incidents such as e-mail abuse, internet misuse, illicit activities, etc. may work to justify the funds spent on a lab.

Lab technician is the other position of significant note for this lab. Technicians must and will have sufficient training to perform their assigned tasks. Some of the skills necessary for the position include – extensive hardware/software knowledge, including OSs and file types, as well as deductive reasoning. Lab technician work is to be assessed accordingly by the lab manager and peers to ensure quality on a regular basis. Lab technicians are also required to continuously engage in technical training to update their investigative and computer skills, along with maintaining a record of said training that they have successfully completed.

Lab technicians are to review digital information relating to criminal investigations. The main task for the technician is to analyze computers as well as audio,

video and other digital devices to uncover information that may assist in the prosecution of suspects and bad actors. It is very much custom for lab technicians to work irregular hours, and they may even get called in to prepare materials for court cases, testify in court and further analyze evidence. Behind the lab manager is the lab technician in their importance to forensic lab facility operations.

Other miscellaneous positions pertain to security, sanitation, and maintenance. All security personnel are expected to provide a physical presence as well as monitor visitor logs and traffic – ensuring the integrity and security of all evidence and staff. Sanitation crew members are expected to maintain complete cleanliness of the facility with a large emphasis on eliminating excess dust buildup that may corrupt evidence and disrupt proper ventilation. Maintenance staff members will be needed on an on-call basis, prepared to come in at moment's notice and provide the proper repair or replacement needed in a relatively timely manner.

Audit Procedure

Staff will conduct inspection of the lab's ceiling, floor, roof, and exterior walls at a minimum of once a week, looking for anything unusual or new. Part of the process will also entail inspection of doors to make sure they close and able to lock properly. Locks will be examined to determine whether they need to be replaced or changed. Security personnel is expected to regularly review visitor logs to observe whether or not they are being used correctly. Security also will routinely examine log sheets of evidence containers to determine when they have been opened and closed. Any evidence that's not being processed on a forensic workstation will be properly secured at the end of every workday.

Calibration

Equipment and all other supplies will be maintained in an organized, pristine, and secure condition. Lab facility inventory will be handled responsibly to ensure optimal performance and in avoidance of any potential contamination, excessive wear and damage. It is the responsibility of the lab manager to ensure that proper planning and care is taken in the event of any equipment, tools, instruments, or evidence. Inventory requiring movement to a manufacturer/vendor for calibration or maintenance will be shipped with maximum care as to eliminate the possibility of damage in transit. Any infrequently used equipment shall be stored, as well as powered down and covered accordingly per the manufacturer's recommendations. Preventative maintenance steps are to be taken by professionals at the beheads of the lab manager as to ensure optimum performance from the equipment – such as performing a Windows update on each computer. Such action is then to be documented on the Computer Maintenance Log for the computer it was performed on.

Work Cited

"ISO/IEC 17025:2017(En) General Requirements for the Competence of Testing and Calibration Laboratories." *ISO*, ISO/IEC, www.iso.org/obp/ui/#iso:std:iso-iec:17025:ed-3:v1:en. Accessed 21 Feb. 2024.

"What Is ISO 17025 Accreditation?" *Campbell Scientific*, www.campbellsci.ca/why-is-iso17025-calibration-important. Accessed 20 Feb. 2024.

Nelson, Bill, et al. *Guide to Computer Forensics and Investigations: Processing Digital Evidence*. 6th ed., CENGAGE LEARNING, 2018, *Cengage*, Accessed 20 Feb. 2024.

"Digital Forensics Careers: Salary Info & Job Description." *Learningpath.Org*, learningpath.org/articles/Digital_Forensics_Careers_Salary_Info_Job_Description.html. Accessed 20 Feb. 2024.

Digital Evidence Quality Manual, www.dps.arkansas.gov/wp-content/uploads/2020/05/Digital-Evidence.pdf. Accessed 20 Feb. 2024.