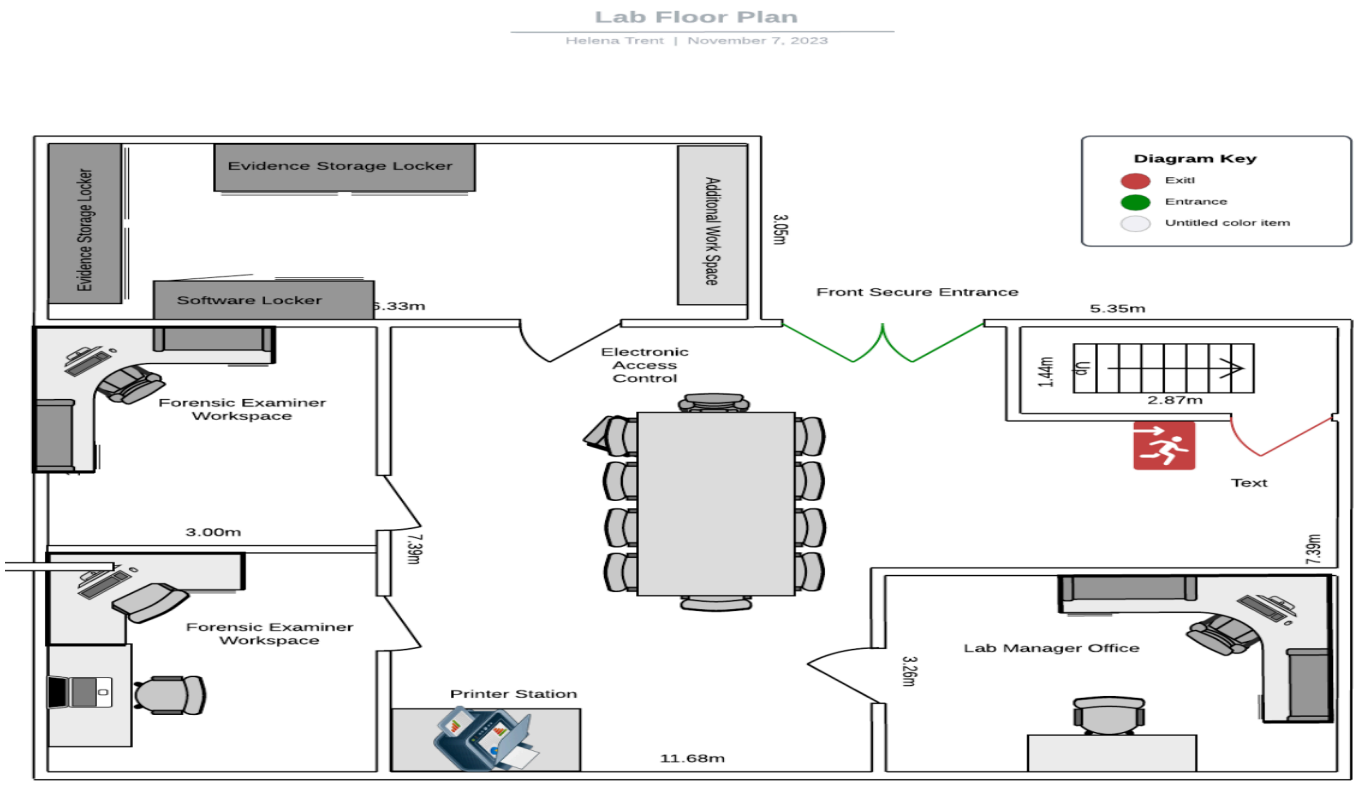
Floor Plan Diagram



Equipment & Facility Security

Workspaces should function as evidence lockers during an analysis. To ensure integrity all spaces in the lab will be locked and utilize an electronic access control system. This means that identification cards will be needed to access all spaces including enclosed workstations and storage rooms. Employees will be granted access depending on their position and there will be a running log on all uses of id cards in case of incident. All visitors that do not possess an identification card will be required to sign in on a visitation log. Visitors will also be required to wear a visible visitors badge displaying their identity while in the lab for proper identification. The lab will also be up to TEMPEST standards to ensure that there is no eavesdropping on the lab which would break integrity.

Equipment Needed

Software:

- Wireshark
- Kali Linux
- Helix Pro
- Cloud Storage
- Firewalls
- Antivirus/Virus Protection Software (McAfee, Symantec)

- Autopsy
- FTK
- OSforensics
- Encase
- Assorted Programming Languages
- Microsoft Office
- Accounting Applications

Hardware:

- Printer
- Workstations
- Cisco 3560 Switch
- Cable Tester
- Spectrum Analyser
- Hardware Write Blocker
- Large Monitors
- Speakers
- Routers
- Assorted adapters/power connecters
- Computer Hand Tools
- External CD/DVD Drive
- Various Hard Drives
- Digital Camera
- Antistatic Bags

Lab Accreditation Plan

This lab will follow the ANAB accreditation plan. First the lab needs to obtain a quote from the accreditation board and submit an application. While this process is happening the lab needs to be in pristine condition to ensure that all necessary equipment and practices are in place at the time of assessment. After the assessment, follow-up, and review the decision on accreditation will be made. After the accreditation is obtained the lab will be under surveillance and reassessed periodically. In addition the lab will have to complete mandatory audits to keep their accreditation through the ANAB. It is the lab managers responsibility to stay on top of the accreditation assessments and audits as it is the livelihood of the lab.
https://anab.ansi.org/accreditation/iso-iec-17025-forensic-calibration/

Lab Maintenance Plan

The lab should be maintained according to this maintenance plan at all times to ensure the safety of lab personnel and material kept within the lab. Employees, especially lab managers, should be vigilant and conduct routine maintenance sweeps. Any damages to floors, ceilings, walls, etc should be reported immediately and fixed within a timely manner. The temperature of the laboratory should be approximately 70 degrees fahrenheit to assure the comfortability and safety of personnel and equipment.

Software Maintenance:

Software should be updated regularly according to the manufacturer. There should be regular checks to ensure that software is operating properly. Staff should be adequately trained to the point of familiarity with all software being used during examinations. Staff who are not familiar with software being used on a case are not permitted to work on those specific cases and should be supervised and trained by a manager.

Hardware Maintenance:

Hardware should be checked regularly for anything that may impact performance. This could include bent wires, normal wear and tear, speed of machines, etc. If hardware is found to be damaged or defective it should not be used and replaced as soon as possible.

Cleaning:

The lab should be cleaned once a week by professional cleaners hired by the lab. Cleaners should be instructed to focus on eliminating dust in the lab by thoroughly mopping and vacuuming spaces. A trash system should be put in place that separates sensitive materials from regular trash and cleaners should be aware of this. A company who specializes in disposal of sensitive materials should handle the trash to avoid discarded information from being viewed by unauthorized individuals.

Job Descriptions

Lab Manager:

This is a managerial and supervisory role. Major responsibilities include administrative tasks and team leadership. As manager the individual in this role will be responsible for a team of forensic technicians. Acting managers will review and plan the work of those under their supervision. In addition lab managers will be expected to be able to perform complex and advanced casework and advise technicians accordingly. Lab managers in this facility also conduct the annual reaccreditation assessments as required by the ANAB. Occasional field work can be expected in this role including court appearances.

- This position requires experience with digital forensics hardware and software tools. Some technical skills and responsibilities include …
    - Recovering deleted and/or encrypted data
    - Preserving original media
    - Establishing ownership for evidence purposes
    - Familiarity with MAC, Linux, and Windows systems
    - Accessing password protected files
    - Presentations and reports on findings
    - Familiarity with chain of custody
    - Providing expert testimony when needed

Preferred Experience & Education

- 5+ years of relevant experience reaching an advanced or expert level
- Project management experience
- Possess at least one professional certification
- Bachelor's Degree in related field or equivalent experience
- Certifications (GIAC, CFCE, CCFP, CCE)

Lab Technician:

Conduct digital forensic analysis and meet lab requirements. Although this position is not a supervisory role, there will be situations where jr lab technicians will need assistance and guidance. It also may result in the delegation of tasks to jr technicians working in the lab. The individual in this role will be expected to adhere to lab procedures and maintain chain of custody when necessary. In addition technicians are responsible for maintaining the forensic library and properly storing evidence. Occasional field work can be expected and work from home is not an option.

- This position requires experience with digital forensics hardware and software tools. Some technical skills and responsibilities include …
    - Recovering deleted and/or encrypted data
    - Preserving original media
    - Establishing ownership for evidence purposes
    - Accessing password protected files
    - Familiarity with chain of custody
    - Prepare written documentation

Preferred Experience & Education

- 1 year of relevant experience or more
- Associates degree in relevant field (i.e Computer Science,Cyber Security,Cyber Crime, etc)
- Certifications (GIAC, CFCE, CCFP, CCE)
- On the job training and professional development opportunities while employed

** Degree requirements can be satisfied by work experience and proper certifications**