Accreditation Plan

The laboratory will pursue accreditation under the ISO/IEC 17025:2017 standard through the following steps:

1. Purchase a licensed copy of the ISO/IEC 17025 document, be in possession of the MA 3033 accreditation manual, and be in possession of the AR 3125, AR 3120, and AR 3181 documents ("Accreditation Manual for Forensic Laboratories," 2024).
2. Create a draft scope for the laboratory's accreditation, and complete an electronic formal application for accreditation, which are both to be submitted to ANAB ("Accreditation Manual for Forensic Laboratories," 2024).
3. Communicate with the relevant assessors to plan the date and timeframe in which the ISO/IEC 17025:2017 compliance assessment will occur, ensure all necessary documents prior to the assessment have been provided, and communicate any other considerations ("Accreditation Manual for Forensic Laboratories," 2024).
4. Ensure the laboratory is in compliance with all appropriate aspects of ISO/IEC 17025:2017 and retain documentation of this compliance. This includes:
    - Comprehensive and up-to-date documents related to the activity of the laboratory and the requirements placed upon it.
    - An organization chart, demonstrating the line of authority within the organization, or who holds authority over others ("Accreditation Requirements for Forensic Inspection," 2023). The laboratory manager should hold authority over all other laboratory employees, with other authority relationships at the discretion of the laboratory manager.

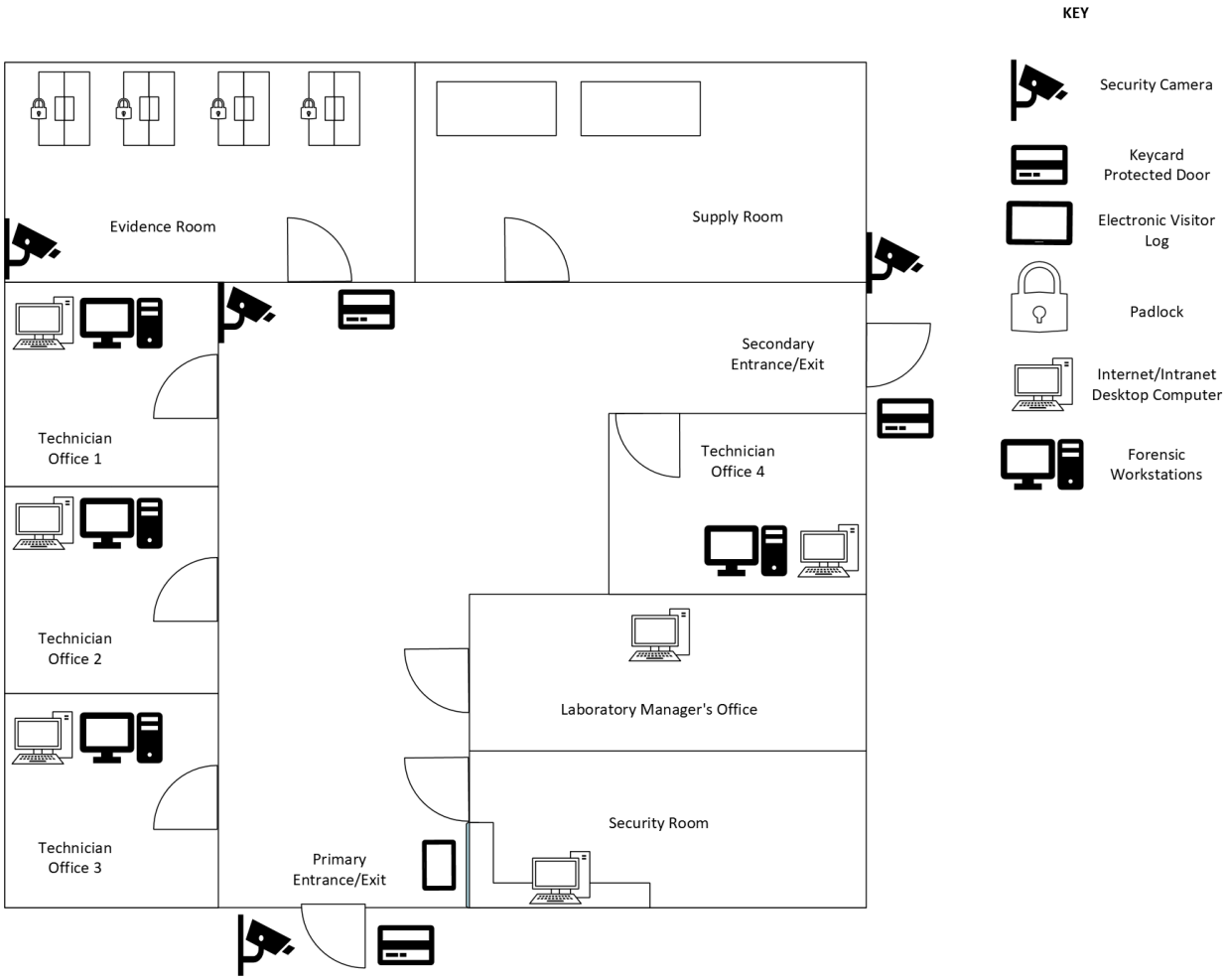
- Internal auditing. The laboratory should conduct its own review of its capabilities and attributes in relation to the requirements laid out in ISO/IEC 17025:2017 and its own policies to determine its overall compliance ("Accreditation Requirements for Forensic Testing and Calibration," 2023).
- Preventive actions. If certain aspects of the laboratory and its functioning are found to be in noncompliance with one or more areas of the ISO/IEC 17025:2017 standard, steps should be taken to resolve these issues before assessment occurs. These should be documented.
- Proof of corrective actions. Should the laboratory be found to be noncompliant in one or more areas, steps shall be taken to eliminate the cause of this nonconformity, allowing for compliance to be confirmed during the assessment or reassessment. These procedures must identify the cause of the nonconformity, take steps to eliminate the nonconformity, and determine whether these steps were successful ("Accreditation Requirements for the Management and Operation of Property and Evidence Control Units," 2023).
- Management reviews. The laboratory should, on an annual or bi-annual basis, review its policies, goals, and productivity, alongside other internal and external feedback, in order to determine if changes in the management of the facility are necessary or beneficial ("Accreditation Requirements for the Management and Operation of Property and Evidence Control Units," 2023).
- Documentation of proficiency testing. This involves comparisons with external testing organizations. Testing the abilities of employees and the laboratory as a

whole allows their results to be significantly more trustworthy (“Accreditation Manual for Forensic Laboratories,” 2024).

- Quality Assurance (QA) reports. Much like proficiency testing, QA reports allow the laboratory to validate the accuracy of their tools and processes.
- Appropriate facilities. This involves a building permitting investigations to be carried out reliably, securely, and safely. As shown below in the facility diagram, the facility should meet the physical requirements of ISO/IEC 17025:2017.
- Documentation of the methods by which devices and data will be tested or examined. Reliable and validated methods are necessary to ensure the accuracy of investigation outcomes.
- Traceability. The traceability of results involves their connection, through calibrations, to a trusted source (“Accreditation Requirements for Forensic Testing and Calibration,” 2023). Any device or application must be calibrated by another entity, such as another accredited laboratory, which itself has been properly evaluated (“Accreditation Requirements for Forensic Testing and Calibration,” 2023). The chain of calibrations by which the laboratory’s equipment has been verified must be documented.
- The laboratory should account for the uncertainty of measurements. Any factors that might contribute to inaccuracies in measurements made by the laboratory should be recognized, and their impact documented (“Accreditation Requirements for Forensic Testing and Calibration,” 2023).

5. Complete an ANAB conformance checklist, using the documentation outlined in step four, and send this document to ANAB, at a minimum, 45 days before the assessment is scheduled to occur ("Accreditation Manual for Forensic Laboratories," 2024).
6. Meet with the ANAB accessor(s) and begin the assessment. Employees should be available to answer questions asked, and documents related to the laboratory's specifications and functioning should be prepared ("Accreditation Manual for Forensic Laboratories," 2024).
7. Resolve any compliance oversights within one month of the assessment and report these changes to ANAB, if this becomes necessary ("Accreditation Manual for Forensic Laboratories," 2024).

Laboratory Diagram



Staffing

Laboratory Manager

Requirements:

The laboratory manager should possess at least moderate experience with many kinds of devices and operating systems, including Windows, Macintosh, Linux, and mobile environments, and should have a strong understanding of how digital forensics investigations are carried out. The laboratory manager should have strong leadership and communication skills, in order to effectively designate tasks to technicians and

employees and further organizational objectives. At least five years of experience as a digital forensics investigator or a similar position is required for this role. At a minimum, the laboratory manager should have obtained two or more appropriate certifications from reputable organizations, such as the IACIS's "Certified Forensic Computer Examiner" certification, the "Certified Cyber Forensics Professional" certification from ISC², and the "Certified Computer Crime Investigator, Advanced" or "Certified Computer Forensic Technician, Advanced" certifications from the High Tech Crime Network (Nelson et al., 2017). A degree in Computer Forensics or a similar field is also preferable.

The duties the lab manager must perform are as follows:

- Create, implement, and communicate policies related to the appropriate processes for investigations, to ensure a productive work environment is created which complies with the relevant legal and regulatory requirements (Nelson et al., 2017). Such policies will relate to evidence collection and preservation, evidence handling and logging, documentation of activities, evidence storage, and reporting specifications (Nelson et al., 2017).
- Monitor employee activity to ensure policies are followed, and enforce ethical standards among employees (Nelson et al., 2017).
- Determine and delineate appropriate schedules for cases as they are acquired, given the preliminary information that is available and their own knowledge about the laboratory's capabilities (Nelson et al., 2017).
- Regularly review the facility's finances, organize upgrades, replacements, or other purchases where necessary (Nelson et al., 2017). Expenses should be managed to allow for financial stability.

- Manage onboarding and facilitate appropriate training for new employees, if key laboratory positions are unfilled, manage offboarding for employees ending their employment at the laboratory, and carry out disciplinary actions, if necessary.

Technician - Windows Specialist

Requirements:

Technicians specializing in Microsoft Windows systems should have significant experience working with various versions of the Windows operating system, and must be competent in evidence collection and analysis in these environments. They should possess strong reasoning skills, allowing them to effectively analyze and report on any evidence found. A thorough understanding of computer hardware as it relates to digital forensics is also necessary. In addition, this technician must have the relevant certification for forensic investigations of Windows systems, such as IACIS's Certified Advanced Windows Forensic Examiner certification or an equivalent certification (Nelson et al., 2017). A degree in Computer Forensics or a similar program, and prior experience in digital forensics, are also recommended.

The duties this technician must perform are as follows:

- Collect digital evidence from systems and drives as directed. The technician must do so while taking measures to protect evidence from unintentional alterations.
- Analyze digital evidence through the use of GUI and command-line applications.
- Create reports on findings, clearly communicating what was found and how it relates to the case at hand.
- Testify in a court of law about their activities and findings, as necessary.
- Continue to build skills in digital forensics in order to remain competent as new devices, operating systems, and other software are released, with a focus on Microsoft Windows.

Technician - Mac Specialist

Requirements:

Technicians specializing in Macintosh systems should have a high degree of past experience working with various iterations of macOS, and must be competent in evidence collection and analysis on these systems. They should possess strong reasoning skills, allowing them to effectively analyze and report on any evidence found. A high degree of knowledge in computer hardware as it relates to digital forensics is needed, as well. Further, this technician must have the relevant certifications proving competency in digital forensic investigations involving Macintosh systems, such as SUMURI's "Certified Forensic Mac Examiner" certification or some certification that is equivalent (*Mac Forensics Certification Program*, n.d.). A degree in Computer Forensics or a similar program, and prior experience in digital forensics, are also recommended.

The duties this technician must perform are as follows:

- Collect digital evidence from systems and drives as directed. The technician must do so while taking measures to protect evidence from unintentional alterations.
- Analyze digital evidence through the use of GUI and command-line applications.
- Create reports on findings, clearly communicating what was found and how it relates to the case at hand.
- Testify in a court of law about their activities and findings, as necessary.
- Continue to build skills in digital forensics in order to remain competent as new devices, operating system versions, and software are released, with a focus on macOS.

Technician - Linux Specialist

Requirements:

Technicians specializing in Linux systems should have a good deal of prior experience working with various distributions of Linux and UNIX, and must be able to effectively collect and analyze evidence present on these systems. They should possess strong reasoning skills, allowing them to effectively analyze and report on any evidence found. In addition, a high degree of knowledge in computer hardware as it relates to digital forensics is needed. Further, this technician needs a relevant certification proving competency in digital forensic investigations involving Linux systems, such as Cyber5W's "Certified Linux Forensic Analyst" certification, or other certifications that can fulfill this requirement (*Linux Forensic Analyst Exam*, n.d.). A university degree in Computer Forensics or an equivalent degree, and past experience in the digital forensics field, are also recommended.

The duties this technician must perform are as follows:

- Collect digital evidence from systems and drives as directed. The technician must do so while taking measures to protect evidence from unintentional alterations.
- Analyze digital evidence through the use of GUI and command-line applications.
- Create reports on findings, clearly communicating what was found and how it relates to the case at hand.
- Testify in a court of law about their activities and findings, as necessary.
- Continue to build skills in digital forensics in order to remain competent as new devices, operating system versions, and software are released, with a focus on Linux and its various distributions.

Technician - Mobile Specialist

Requirements:

Technicians specializing in mobile environments, such as those present on cellphones and tablets, should have significant experience working with various versions of the iOS and/or Android operating systems, and must be competent in evidence collection and analysis in these environments. They should possess strong reasoning skills, allowing them to effectively analyze and report on any evidence found. A high degree of understanding in regard to mobile hardware is also crucial. In addition, this technician must have the relevant certification for forensic investigations of mobile devices, such as IACIS's "Certified Mobile Device Examiner" certification (Nelson et al., 2017). A degree in Computer Forensics or similar field, and prior experience working in digital forensics, are preferred.

The duties this technician must perform are as follows:

- Collect digital evidence from mobile systems and drives as directed. The technician must do so while taking measures to protect evidence from unintentional alterations.
- Analyze digital evidence through the use of GUI and command-line applications.
- Create reports on findings, clearly communicating what was found on these devices and how it relates to the case at hand.
- Testify in a court of law about their activities and findings, as necessary.
- Continue to build skills in digital forensics in order to remain competent as new devices, operating systems, and other software are released, with a focus on iOS and Android environments.

If possible, one or more technicians should have training and certification in dealing with hazardous materials, as well. If not, outside HAZMAT teams may need to be consulted and

coached in order to safely collect evidence, in the event that this evidence is otherwise too dangerous to acquire (Nelson et al., 2017).

Laboratory Security

Requirements:

The lab's security guard should be physically and mentally capable of preventing unauthorized individuals from entering the laboratory. They should possess the proper training to respond to security incidents, and protect persons, evidence, and organizational property. Prior security or law enforcement experience is strongly preferred, as are certifications and degrees related to physical security.

The laboratory's security guard will be responsible for:

- Managing entry into the digital forensics laboratory, and preventing unwanted physical intrusions. This also includes managing keycard access to secure rooms, as directed by the laboratory manager.
- Checking in any guests, ensuring that their presence in the lab has been logged appropriately.
- Accompanying guests during their time in the laboratory, if necessary.
- Monitoring activity in and around the lab for suspicious behavior, both physically and through security systems.
- Securing entrances and exits to the laboratory at the end of the workday.

Inventory List

Physical Items/Hardware

Computer Desks (4) & Office Desks (2)

Computer Chairs (4) & Office Chairs (2)

Forensic Workstations (4)

Normal Desktop Computers (6)

Computer Monitors (10)

Computer Mice (10)

Headphones/Earbuds (10)

Mousepads (10)

Keyboards (10)

Power Cables (10)

CAT6/CAT6A Ethernet Cables (15)

ATA Cables (8)

Ribbon Cables (2)

Various Other Adapters & Cables (i.e. USB male-male adapters, USB male-female adapters, USB-C adapters, MicroUSB adapters, HDMI/VGA/DisplayPort cables, etc.)

Surge Protectors (6)

CD/DVD Drives (4)

SCSI Cards (4)

Various Hard Drives

Various USB Flash Drives

Hardware Write Blockers (6)

Antistatic Pads (6)

Laptop Workstations (2)

Electronic Guest Log (1)

Keycard Reader/Lock Mechanism (3)

Keycard Printer (1)

Stationary

Paper Clips & Binder Clips

Manilla Folders/Envelopes

Writing Utensils (Pencils, pens, highlighters, markers, etc.)

Computer Toolkits (6) (Including precision screwdrivers, wrenches, flashlights, antistatic straps, etc.)

Antistatic Evidence Bags (30+)

Regular File Cabinets (6)

Evidence Lockers/Cabinets (4)

Padlocks (4)

Digital Camera (2)

SD Cards (4)

Security Cameras (4)

Operating Systems, Forensic Applications, & Miscellaneous Software

Licenses for Windows 11, 8, 7, XP, 95, and other versions of the operating system, both those built for clients/home use, and those built for servers.

Licenses for macOS, OSX, and older versions of Mac OSs

Kali Linux, Ubuntu, Mint, Debian, and other Linux distributions

Microsoft Word, Microsoft Excel, Microsoft Powerpoint, and other Office applications

Python, JavaScript, C++, and other programming languages

PDBlock

FTK Imager

Autopsy

EnCase

OSForensics

ProDiscover Incident Response

DiskDigger

Wireshark

dcfldd/dc3dd

SMART

Helix 3

Maintenance Plan

A maintenance plan is critical to ensure that devices, equipment, personnel, and the laboratory as a whole remain functional and effective. The following maintenance procedures will allow the laboratory to remain up to date and capable of supporting necessary investigative processes.

Laboratory Examinations

Regular physical checks of the premises are to be conducted by the lab manager or a designated employee at least once each week. These examinations are to include the laboratory's exterior and interior walls, ceilings, the locking mechanisms on each door, and facility lighting and electrical systems. Any physical breakage of the laboratory is to be resolved as quickly as is possible, no more than one week after the irregularity is detected. Should any component of the laboratory require maintenance procedures that are outside of the skillset held by the laboratory's staff, such as electrical complications, an external party is to be contacted to resolve the issue

more effectively. It is critical that, in such a case, the presence of these individuals is logged and their activity is monitored to ensure compliance with laboratory safety and security policies.

Record Keeping

Policies and procedures will be put in place to facilitate record keeping of all items held and purchased by the laboratory. Records will include the name and brand of the item, the quantity owned, and a unique identifier, among any other notable attributes. Doing so will allow lost or stolen items to be identified more readily, ease the process of purchasing replacements, and ensure that the appropriate calibration can occur on all relevant items.

Updates & Acquisitions

Potential software and hardware acquisitions are to be explored annually. Licenses for both new and older operating systems, additional tools and equipment, and forensic software, if not already owned, should be examined to determine if their benefit is greater than the cost to the laboratory. Patches and updates to forensic software are to be done no more than one week after they are available. Funding should be allocated to replace technical components once per year, even if devices show no signs of deterioration. Doing so will allow laboratory infrastructure to function reliably, or for funds to be immediately available for replacements, when systems do inevitably fail. If critical components, for whatever reason, break before this time, replacements are to be purchased no more than two days afterward.

Testing and Calibration

Testing and calibration should be performed via the appropriate methods, as determined by the manufacturer or other authoritative body. Calibration policies for each device will be decided on a case-by-case basis, but no the time period between separate testing and calibration processes should be no more than two months. Both the precise methods in which devices should be tested

and calibrated, and the frequency at which these processes should occur, will be documented as laboratory policy. Equipment, if experiencing major complications, should be replaced at the earliest possible point. Devices that have experienced past malfunctions require expensive testing to ensure that their results can be trusted. If confidence in the reliability of a device or piece of equipment cannot be achieved, its use in forensic investigations is to be discontinued.

Equipment Security

All equipment and devices are to remain in the laboratory at all times. The sole exceptions to this are those laptops, toolkits, evidence containers, and other items designated for use in external evidence collection and investigations. Such items should only be used in the process of evidence collection, or when bringing the relevant systems to the laboratory is impossible. The entrances to the laboratory are to be closely monitored, with surveillance cameras in place near each entrance and the evidence room. Keycard mechanisms are also to be utilized within the entrances to the laboratory and its evidence room. Further, only authorized personnel may handle laboratory equipment. Any alterations made to a device by laboratory staff, which exceed those carried out through the normal use of the device, must first be approved by the laboratory manager. These proposed changes are to be reviewed thoroughly to ensure that they will not inhibit the reliability of the system’s results.

References

Accreditation manual for forensic laboratories, forensic inspection bodies, and property and evidence control units. (2024). In *ANSI National Accreditation Board* (MA 3033). Retrieved October 12, 2025, from https://anab.qualtraxcloud.com/ShowDocument.aspx?ID=7183

Accreditation requirements for forensic inspection. (2023). In *ANSI National Accreditation Board* (AR 3120). Retrieved October 12, 2025, from https://anab.qualtraxcloud.com/Showdocument.aspx?ID=14476

Accreditation requirements for forensic testing and calibration. (2023). In *ANSI National Accreditation Board* (AR 3125). Retrieved October 12, 2025, from https://anab.qualtraxcloud.com/ShowDocument.aspx?ID=12371

Accreditation requirements for the management and operation of property and evidence control units. (2023). In *ANSI National Accreditation Board* (AR 3181). Retrieved October 12, 2025, from https://anab.qualtraxcloud.com/showdocument.aspx?ID=28610

Linux Forensic Analyst Exam. (n.d.). CYBER 5W. Retrieved October 11, 2025, from https://academy.cyber5w.com/courses/c5w-linux-forensic-analyst-exam

Mac Forensics Certification Program. (n.d.). SUMURI. Retrieved October 11, 2025, from https://sumuri.com/mac-training/mac-forensics-certification-program/

Nelson, B., Phillips, A., & Steuart, C. (2017). *Guide to computer forensics and investigations (6th ed.)*. Cengage Learning.