****

**Course: CYB304**

 **IT Security Forensics
(Canadian Context)**

 **Lab 2: Investigator’s**

**Office and Laboratory**

 **Instructor:**

 **Muhamma Saleem**

**Student Name: Olushola Enoch Bayode**

**Student ID: 23077087**

**Section: 3rd Semester**

 **Activity 2-1:**

 For a digital forensics lab to function well, there must be a thorough policies and guidelines document to guide the personnel. For such a document to be a success, we can use the standardized approach which is compliant with standards and best practices below to guide the creation of such a document.

 1. Introduction • Goal: Describe the organization's goals for the digital forensics lab, in the light of its role in reporting, evaluating, and preserving digital evidence. • Scope: Tell us about the range of services that you offer such as video and image analysis, computer and mobile device analysis, and any other technical forensic tasks that you may undertake.

 2. Structure of Organizations • Duties and Positions Held: Establish the main organizational structure of the lab and assign non-overlapping responsibilities to each position, from forensic analyst to lab director. • Training and Competency: To ensure staff members remain competent, provide requirements for continuous learning and competency assessments through established policies.

3. Facilities and Security

Physical Security: The laboratory could employ flawless security measures to restrict the area for people who have no business being there, allowing only those with proper access.This encompasses secure entry systems and visitor logs as well.

Environmental Controls: With regards to the safety of the digital evidence, environmental controls cover maintaining the appropriate environmental conditions such as temperature and humidity.

4. Evidence Handling and Chain of Custody

Evidence Intake: Evidences Intake - Guidance provides a standardized procedure for the receipt of evidence including performing documentation and initial assessment

Chain of Custody: A reliable system must be created to be able to verify evidence movements from the source to the court to the final disposition status, keeping the evidence stored securely and accountable at all times.

Storage: It is important to have a secure storage place for the data that protects it from any damage, loss, or unauthorized access.

5. Examination Procedures

Standard Operating Procedures (SOPs): One such SOP (Standard Operating Procedure) includes Making of a Chain of Circumstantial Evidence, which is among the projects with the highest technical risk but the greatest potential benefits.

Documentation: A detailed record of any analysis performed, including initial and final assessments and the complete process is captured.

6. Quality Assurance

Internal Audits: Organizations carry out a series of assessments to ensure that they comply with their established protocols. As a result, they are capable of finding areas for improvement if there are any.

Proficiency Testing: Testing one's abilities and efficiency by analyzing evidence in a laboratory to become more skilled and no longer make mistakes.

7. Health and Safety

Safety Protocols: Conduct and strictly execute all necessary safety measures for the workers, especially those who are working with hazardous materials.

Emergency Procedures: Lay down a very specific framework for dealing with any unforeseen scenario such as equipment failures, data breaches, or environmental toxins.

8. Legal and Ethical Considerations

Compliance:

 Please, be sure the implementation of activities be consistent with the

 existing laws, rules, and regulations stated by industry.

Ethical Conduct of Forensic Examiner: The forensic analyst needs to focus on conducting the ethical examination by providing transparency, taking clients' opinions into account, and ensuring uninterrupted research.

9. Continuous Improvement

Feedback

 Mechanisms: The management can show that they value the stakeholders' thoughts and perceptions by giving them the opportunity to express their opinions and feelings about the company's performance.

Policy Review: The company will not stagnate but will continue to be aware and active regarding the frequency of policy and procedural reviews necessary for it to remain competitive in the industry in terms of the coverage of the latest technologies and best practices.

References

"Digital Evidence Policies and Procedures Manual" by the National Institute of Justice is the first document that should be read before setting any other policy of the lab from the investigators.

<https://nij.ojp.gov/library/publications/digital-evidence-policies-and-procedures-manual?utm_source=chatgpt.com>

The "Digital Forensic Procedures Manual" by the Indiana State Police is adopted as a service manual and provides guidelines for implementation of information in service, drafting, and using these policies to support the creation.

<https://www.in.gov/isp/labs/files/Digital_Forensic_Procedures_Manual.pdf?utm_source=chatgpt.com>

The Scientific Working Group on Digital Evidence (SWGDE) provides standard operating procedures that serve as a model report that includes the best practices in the investigation field and other related SOPs and guidelines that can be tailored to your laboratory's precise needs. <https://irisinvestigations.com>

Activity 2-2

**GIAC Advanced Smartphone Forensics (GASF) Certification**

**Offered by:**

The Global Information Assurance Certification (GIAC), a worldwide-acclaimed certification body with emphasis on cyber security and digital forensics, provides the GIAC Advanced Smartphone Forensics (GASF) certification. GIAC is a fund of popular practical and theoretical exams that help the student hands-on experience in various cybersecurity domains.

**Overview:**

The GASF certification is oriented to guide the forensic investigators to the specialized skills that are needed for the analysis, and extraction of the digital evidence from the smartphones, and the mobile devices in this era of advanced mobile technology that criminals increasingly use for illegal activities. Hence, mobile forensics have become a very significant part of digital investigations.

The certification covers:

* Mobile Device File System Analysis: The knowledge to unpack the internal structures of Android and iOS devices.
* Application Data Extraction: Recovering and analyzing the data saved by applications like the messaging apps, social media platforms, encrypted communication tools, etc.
* Device Encryption and Data Recovery: The techniques used to crack the encryption and recover data which is deleted or hidden.
* Network and Cloud Forensics: Discovering the mobile device interactions with cloud storage and remote services.
* Malware Analysis: Recognition and dissection of malicious software aimed at mobile devices.
* Legal and Ethical Considerations: Measures for the forensic procedures to be in compliance with the legal standards and the best practices.
* Digital forensic analysts
* Incident response teams
* Law enforcement officers specializing in cybercrime
* Private investigators handling mobile forensic cases
* Cybersecurity professionals dealing with mobile security incidents

Prerequisites:

Although there are no hard and fast prerequisites, it is highly preferable if candidates have some prior experience in the areas of digital forensics, cybersecurity, or incident response. Prospects of the position should be sound in familiar with the principles of forensic methodology and tools of the trade including:

File system analysis

Mobile device data acquisition techniques

Basic scripting and command-line usage

Familiarity with forensic tools like Cellebrite UFED, Oxygen Forensics, and Magnet AXIOM

Details of the Exam:

Format: Multiple-choice questions and the practical scenario-based questions are the two alternatives

Duration: It generally lasts for 2-3 hours; minimum is 2 hours and max. is 3 hours

Number of Questions: Usually more or less 75

Passing Score: It might be different as per the version of the exam

Recertification: Must be renewed every four (4) years

More Information:

**For detailed information, registration, and study materials, visit the GIAC website:**[**https://www.giac.org/certification/advanced-smartphone-forensics-gasf**](https://www.giac.org/certification/advanced-smartphone-forensics-gasf)

**Activity 2-4**

* Disaster Recovery Plan for Digital Forensics Lab
* Company Name: ForensicTech Solutions
* Date: 3/18/2025
* Plan Version: 1.0
* Prepared by: [Your Name]
* Position: Forensic Manager
* Introduction
* A tangle, really thronging the likewise.
* This Disaster Recovery Plan (DRP) defines the procedures and protocols which ForensicTech Solutions will follow to restore digital forensics lab systems and data in case of a disaster. The digital forensic lab is our company's most important infrastructure consisting of forensic testing and the breaking task of password cracking of users. Hence, it is really necessary to do a full and complete system restore whenever there is any loss so that the company will not get disrupted and business will be kept in smooth run.
* Objective
* This strategy is designed to recover and rebuild essential systems and data within a digital forensics lab rapidly in case of a disaster so that the number of interruptions would be minimized and the integrity of the forensic data can be maintained.
* Backup Strategy

Backup Frequency

* Daily Backups: Full backups of all systems, including configurations installed software, and user data, will be conducted every night at 11:00 PM.
* Weekly Backups: A full system backup will be conducted every Sunday, which will include a comprehensive snapshot of all configurations, files, and software installations.
* Monthly Backups: A full backup will be performed at the end of every month and stored offsite to safeguard against long-term data loss.
* Backup Types
* System Image Backups: To restore the system as a whole, the disk image files will be generated by Acronis True Image, or Clonezilla it, including the OS, programs, and settings.

Backup Storage Locations

•Incremental Backups: Incremental backups of sensitive data such as case files, hashes, and analysis output will be performed between the full backups using tools such as rsync on Linux.

•Cloud Backups: Sensitive forensic information will be duplicated to a secure cloud service (e.g., AWS S3, Google Cloud Storage) for geographic redundancy.

•Onsite Storage:

* Network-attached storage devices or external hard disks with the backup disks will be stored in a waterproof and fireproof case inside a locked cabinet within the laboratory.
* The automatic backing up will be programmed regularly so that it would run on a periodic basis.
* The real-time mirroring of sensitive case files to an external NAS device will be done through the central lab storage server.

•Offsite Storage

* A secondary, encrypted copy will be stored offsite at a secure facility (e.g., an external data center or partner facility) for geographic redundancy.
* Cloud backups will also have an added guarantee of trust, offering access to data even in the case of physical destruction at the primary site.
* Programs and Operating Systems
* Operating Systems Installed

• Linux (Ubuntu 20.04 LTS): Deployed as the default operating system in most of the password-breaking and forensic-analysis computers. Linux is best suited for delivering stability and performance when conducting GPU-enabled password-breaking operations.

• Windows 10/11 Pro: Deployed in those computers where administrative work, reporting, and forensic analysis require running Windows-specific tools.

• macOS: Deployed on one computer only to carry out some forensic activities on macOS-only.

* Key Programs Installed Forensic Software:

o Autopsy (open-source hard drive forensic digital forensic tool for examination)

o FTK Imager (for disk imaging)

o EnCase Forensic (forensic evidence collection and analysis)

o Wireshark (network traffic analysis)

o X1 Social Discovery (social media forensic analysis)

• Password-Cracking Tools:

Hashcat (GPU-based password-cracking tool)

John the Ripper (alternative password-cracking tool)

Cain and Abel (Windows password recovery tool)

• Security Tools:

Snort (Intrusion Detection System for network traffic analysis)

Wireshark (network packet capture and analysis)

• System Monitoring and Backup Tools:

Acronis True Image (for system image backup)

o　Veeam Backup & Replication (for virtual infrastructure disaster recovery management and backup)

Backup Software and Cloud Services:

•rsync (for incremental backups on Linux)

•AWS S3 (for cloud storage of the backups)

•Backblaze (for additional cloud-based redundancy for backups)

Disaster Recovery Procedures

Initial Disaster Response

1.Assessment: Immediately identify the nature and extent of the disaster, i.e., what systems are affected (server crash, network breach, fire, flood).

2. Communication: Alert affected stakeholders including the IT division, department management, and top executive management, and inform them about the occurrence.

3. Incident Report: Document disaster information on an incident report for potential later use.

Restoration Process

System Prioritized Restoration: Restoration of critical systems. The most significant systems including password-cracking labs, file servers, and forensic analysis lab computers would first be restored.

Recover systems via system images restore in the case of equipment malfunction.

If probable data compromise is likely to occur, restore system integrity and retrieve compromised data from the latest, unaltered backup.

OS and Program Recovery:

 \* OS Reinstallation: Reinstall the OS from the most recent system image backup.

 \* Adding Back Tools: Reteare memory workspace with double NDA according to BJ-SC understanding.

Data Recovery:

 \* Restore backups of vital case files, logs, and data analysis reports.

 \* Revalidation of the data integrity will be carried out after its extraction from backups to ensure that the data corruption problem is solved during its recovery process.

Test Recovery Systems

• Conduct a complete system test after the system recovery and check if all functions are properly enabled. This includes the checking of network connectivity, password-cracking capabilities as well as forensic tools.

Documentation

• Record all steps of the disaster recovery process including recovery time, and difficulties faced, which will be used in the future to improve DRP processes.

Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)

RTO:

• Critical Systems (Password-Cracking Workstations): 4 hours

• Other Systems (Forensic Servers, Admin Workstations): 6 hours

RPO:

• Forensic Data: 24 hours annual data loss, as per the daily schedule.

• System Images and OS Configuration: 7 days of configuration loss, as per weekly schedule.

**Physical and Cloud Backup Storage Locations**

Onsite Backup Storage:

Backup disks (e.g., external USB hard drives) and a NAS device are kept in the secured server room located within the main office building at [Building Address]. The room is kept safe through factors like environmental control, precision suppression units, and 24 hours of surveillance.

Offsite Backup Storage:

Backups were transferred to a building that can withstand disasters, to a data center, whose address in California.

Cloud backups are kept in two places, AWS S3 and Backblaze, for doubling the data to be stored in more than one server.

Conclusion

This disaster recovery solution will get ForensicTech Solutions back in the business very soon after a disaster without tons of throughput for forensic data. Regular testing of the backup systems and recovery processes will ensure that the laboratory will continue to operate in an efficient manner, delivering high-quality digital forensics services.

For further inquiries or clarifications, please contact the IT Department.

**Websites:** Author, A. A. (Year, Month Day). Title of webpage. *Website Name*. URL

Example: Jones, M. (2022, June 15). Best practices for disaster recovery planning in IT. *Tech Insights*. <https://www.techinsights.com/disaster-recovery>