Lab 1

Classification Level	Definition	Examples
Level 5: Restricted	This security level represents the most sensitive data within an organization. Data in this category poses a severe threat if exposed to unauthorized individuals. It includes information like nuclear launch codes, which could have catastrophic consequences if leaked. National security briefings and highly classified research also fall into this category. Protecting and restricting access to this data is of utmost importance to prevent potential harm and ensure the safety and security of the organization and the nation.	• Nuclear Launch Codes, National Security Briefings, Highly Classified Research
Level 4: Confidential	Data classified at this level is highly sensitive and should only be accessed by authorized personnel. Unauthorized exposure of this data can lead to significant harm, such as the disclosure of unreleased medical research cures, trade secrets, or classified business strategies. Organizations must implement strict security measures and access controls to safeguard this information. Breaches at this level can result in substantial financial and reputational damage, making it essential to prioritize its protection and limit access to only those with a legitimate need.	• Medical Research with Unreleased Cures, Trade Secrets, Classified Business Strategies
Level 3: Internal	This security level pertains to moderately sensitive data intended for internal use. While not highly classified, its exposure could have moderate adverse effects. Examples include project plans, internal financial reports, and employee performance data. These documents are crucial for the organization's day-to-day operations and decision-making processes, but they should still be protected to maintain confidentiality and integrity. Ensuring that only authorized personnel can access and handle this data is important to prevent potential leaks or misuse that could harm the organization's internal processes and reputation.	• Project Plans, Internal Financial Reports, Employee Performance Data
Level 2: Limited	Less sensitive data falls under this security level, intended for broader internal use and sharing with authorized external partners. Examples include company newsletters, non-confidential supplier information, and general organizational charts. While unauthorized disclosure may have a low adverse effect, organizations must still	• Company Newsletters, Non-confidential Supplier Information, General Organizational Charts

	exercise caution and control over access to maintain data accuracy and consistency. Ensuring proper handling of this data is essential to prevent potential misunderstandings or errors in communication with external partners and stakeholders.	
Level 1: Public	This security level includes data intended for public disclosure. There is no harm in this data being accessible to anyone, and it typically includes press releases, general company information, and publicly available research findings. While this data is not sensitive, organizations must still ensure its accuracy and consistency to maintain a positive public image and provide accurate information to the public and stakeholders. It plays a crucial role in communication and transparency, allowing organizations to share information openly without compromising security or confidentiality.	• Press Releases, General Company Information, Public Research Findings

Lab 2-5: Data Handling Requirements Matrix

Creation Table

Activity	Level 1 Public	Level 2 Limited	Level 3 Internal	Level 4 Confidential	Level 5 Top Secret
Access To Customer Data	Providing public access to basic customer information, such as general contact details or product information. This data is intended for open disclosure and does not require special protection.	Allowing limited internal access to customer data for authorized personnel and external partners. This may include customer profiles and purchase history. While not highly sensitive, it must be handled carefully for	Managing internal access to comprehensive customer data for marketing campaigns or customer support. This data is moderately sensitive and essential for internal decision-making and customer interactions.	Controlling access to highly sensitive customer data, such as financial information, social security numbers, or confidential contracts. Strict security measures and access controls are vital.	Handling top-secret customer data, such as national security-related information or highly classified individual records. This requires the highest level of security and access restrictions.

		accuracy and compliance.			
Software Development	Developing public-facing software or applications for general use. These projects are meant for open disclosure and do not require special protection.	Engaging in limited internal software development projects, like creating company intranet tools or software for authorized partners. While not highly sensitive, these projects should maintain data integrity.	Working on internal software development projects for streamlining operations or enhancing productivity. This data is moderately sensitive and crucial for internal processes.	Engaging in highly sensitive software development, such as proprietary algorithms, trade secrets, or classified software projects. Strict security measures and access controls are essential.	Participating in top-secret software development for national security or highly classified applications. This requires the highest level of security and access restrictions.
Data Transfer	Facilitating public data transfers for publicly accessible information, such as public research findings or open-source data sharing. This data is intended for open disclosure and does not require special protection.	Managing limited internal data transfers for authorized purposes, like sharing non-confidential reports with external partners. While not highly sensitive, these transfers should ensure data accuracy.	Overseeing internal data transfers for operational purposes, including sharing project-related information or training materials. This data is moderately sensitive and crucial for internal processes.	Handling highly sensitive data transfers, such as confidential contracts, trade secrets, or classified research data. Strict security measures and access controls are essential.	Managing top-secret data transfers, including national security briefings or classified research findings. These transfers require the highest level of security and access restrictions.

Storage Table

Activity	Level 1 [Public]	Level 2 [Limited]	Level 3 [Internal]	Level 4 [Confidential]	Level 5 [Top Secret]
Storing Data On Local Drives	It is not advisable to use local drives as they lack backup capabilities.	Local drives are prohibited as a storage option.	Local drives are not authorized for data storage.	Local drives are strictly forbidden for data storage.	Local drives are strictly prohibited for any data storage.
On-Premises Storage (Digital)	Employing network drives with no access control and implementing regular backup schedules.	Using encrypted drives with access control lists, and ensuring backups are stored in secure locations.	Establishing restricted network segments with enforced access policies, coupled with robust encryption, and performing daily backups with secure storage.	Operating dedicated servers in secured rooms, enforcing multi-factor authentication for access, and maintaining continuous backups with offsite storage.	Operating isolated servers within air-gapped networks, implementing biometric access control, and achieving real-time backups to undisclosed, secure locations.
Cloud Storage	Utilizing public cloud services for storing data classified as non-sensitive, with no special encryption measures.	Opting for cloud services with encryption at rest and in transit, and limiting access to specific users.	Employing private cloud services with end-to-end encryption, stringent access controls, and comprehensive logging.	Utilizing private cloud solutions with advanced security features, internally managed encryption keys, and regular security audits.	Leveraging highly secure, specialized cloud services, utilizing personalized encryption keys, and limiting access to specific roles and authorized individuals.
Offsite Physical Storage	Using standard, commercially available storage facilities with basic security measures.	Choosing commercial storage facilities with additional security features such as CCTV and access control.	Opting for secure storage facilities with limited access, monitored entry, and alarm systems.	Utilizing highly secure storage facilities with 24/7 monitoring, armed security personnel, and meticulous access logs.	Employing maximum-security facilities with biometric access control, military-grade security protocols, and continuous surveillance.

Portable Storage Devices	Allowing unrestricted use of USB drives, CDs, etc., without the need for encryption.	Employing encrypted USB drives or CDs with registered serial numbers, tracking and logging their use.	Restricting the use of portable storage devices, mandating encryption, and approving usage on a case-by-case basis, with vigilant monitoring and logging.	Implementing highly restrictive policies for portable devices, requiring advanced encryption and case-by-case approval for usage.	Generally prohibiting the use of portable storage devices, with exceptions granted only for extreme cases, involving multi-layer encryption and GPS tracking.

Usage Table

Activity	Level 1 [Public]	Level 2 [Limited]	Level 3 [Internal]	Level 4 [Confidential]	Level 5 [Top Secret]
Accessing Data On Shared Drives	For accessing data on shared drives, users should adhere to standard user authentication practices, including providing a username and password.	At Level 1, users need VPN access to remotely access the data; access from public networks is prohibited.	Level 2 requires two-factor authentication for all remote access; file and folder access is provisioned to select users.	Level 3 involves strict control, limiting access to specific departments, with user access logged and periodically reviewed.	Level 4 prohibits remote access; access is confined to on-site users. No remote access is permitted.
Viewing Data	Viewing data is openly accessible to all employees and the public, with no special authentication requirements.	Access to view data is limited to designated teams, requiring user credentials for login.	Data viewing is restricted to specific departments, with access logged and periodic reviews conducted.	Viewing data is under strict role-based control, requiring two-factor authentication and real-time access logging.	Only a handful of authorized personnel can access and view data, with continuous monitoring and biometric authentication.
Editing Data	Editing data is allowed for all staff with basic privileges, and changes are logged for audit purposes.	Editing rights are limited to authorized personnel, with all changes tracked and subject to audit.	Editing rights are strictly controlled and confined to specific roles, with detailed documentation.	Editing is highly restricted, requiring formal approval and comprehensive logging.	Editing is generally prohibited, allowed only under exceptional circumstances with a full audit trail and senior

					management approval.
Sharing Data Internally	Data sharing internally has no restrictions and can be freely accessed and shared among all staff.	Internal data sharing is restricted to staff within the organization, with sharing actions logged.	Internal data sharing requires managerial approval for sharing outside the immediate team, and records of sharing are maintained.	Internal data sharing is strictly controlled, shared on a need-to-know basis, requiring approval from senior management.	Internal data sharing is generally prohibited, allowed only with approval from executive leadership and detailed justification.
Sharing Data Externally	Data can be freely shared externally without special permissions and is suitable for public dissemination.	Limited data sharing is allowed under specific conditions, requiring approval from the department head.	External data sharing is generally prohibited, except under specific contractual or collaborative agreements.	External data sharing is extremely restricted, requiring executive approval and nondisclosure agreements.	External data sharing is prohibited, except under legal or governmental mandates, and only with the highest level of executive approval.

Transmission Table

Activity	Level 1 [Public]	Level 2 [Limited]	Level 3 [Internal]	Level 4 [Confidential]	Level 5 [Top Secret]
Emailing Data Internally	Follow standard practices aligned with the Email Acceptable Use Policy.	Level 1 requires including a statement identifying the classification level and listing restrictions for redistribution. Ensure proper redactions for open records requests. Verify recipient information to prevent unintentional information disclosure.	Same as Level 2, with data password protection and encryption (password not in the same email). Non-encrypted email transmission is prohibited. Include a statement identifying the classification level and listing redistribution restrictions.	Level 4 additionally requires labeling the email classification in the subject line. Sending Level 5 data should be minimal and approved by the appropriate data owner(s).	Sending Level 5 data must be kept to a minimum and requires approval from the appropriate data owner(s).
Emailing Data Externally	Open for general public information. No restrictions on external email communications . Standard SMTP protocol.	Requires explicit managerial consent. Use encrypted email service. Mandatory inclusion of data sensitivity disclaimer in email body and attachments.	Prohibited for general use. Allowed under specific circumstances with contractual obligations. Encrypted email channels with digital signatures.	Strictly controlled; requires senior management approval. Secure email gateways with features like Data Loss Prevention (DLP). Mandatory use of non-disclosure agreements for recipients.	Generally not allowed; exceptional cases require board-level approval. Utilization of specialized, secure email systems. Real-time monitoring of email transactions.
Data Transfer Over Networks	Unrestricted use of the organization's network for data transfers. Basic encryption like SSL/TLS for web-based transfers.	Encrypted data transfers using VPNs or SSL/TLS. Access and transfer logs are maintained with periodic audits for compliance.	Restricted to secure internal networks with enforced VPN use. Strong encryption standards like AES-256 for data in transit. Detailed transfer logs and regular	Mandatory use of highly secure, encrypted network channels. Restricted transfer protocols, with every transaction logged and	Transfer is restricted to isolated, highly secure networks. Real-time monitoring of all data movements. Pre-approval required for each transfer, with detailed

			security reviews.	audited. Use of network segmentation to control data flow.	justification and top-level oversight.

Archiving Table

Actitivy	Level 1 [Public]	Level 2 [Limited]	Level 3 [Internal]	Level 4 [Confidential]	Level 5 [Top Secret]
Archiving Data To A Backup Provider Or Cloud Service	Ensure that third-party adheres to Level 1 data archiving and storage requirements.	Ensure that third-party complies with Level 2 data archiving and storage requirements.	Ensure that third-party follows Level 3 data archiving and storage requirements.	Ensure that third-party follows Level 4 data archiving and storage requirements.	Ensure that third-party follows Level 5 data archiving requirements.
Archiving Data In The Cloud	Utilize standard, publicly available cloud services, with data tagged for easy retrieval. Conduct annual audits for data accuracy and relevance.	Opt for secure cloud services with client-side encryption, access controls, and key management procedures. Conduct semi-annual data audits for compliance and relevance.	Employ private cloud solutions with end-to-end encryption, regular access reviews, and strict user authentication. Conduct quarterly audits for data integrity and security compliance.	Choose highly secure cloud services with multi-layered security features, data anonymization where possible, and frequent audits for data integrity and adherence to security protocols.	Implement customized cloud solutions with the highest level of security, personalized access controls, encryption key management, and frequent integrity audits, along with continuous compliance checks.
Physical Archiving (Paper, Usbs, Etc.)	Utilize open storage in office environments, with regular disposal and shredding schedules for outdated documents.	Opt for secure storage in locked cabinets or safes, conducting regular audits and controlled disposal processes for outdated media.	Implement restricted storage in access-controlled environments, secure shredding, and disposal protocols for outdated documents, along with	Choose highly secure storage in restricted access safes or secure rooms, with immediate shredding and secure disposal of outdated documents, frequent security audits.	Opt for maximum-security storage in vaults or secure, monitored environments, with specialized destruction methods for outdated documents, continuous surveillance,

			regular audits for compliance.		and strict access logs.
Offsite Archiving	Utilize standard commercial storage facilities, conducting regular audits for data integrity and relevance.	Opt for secure offsite storage with controlled entry and exit logs, regular data integrity checks, and inventory audits.	Choose restricted access offsite storage facilities with enhanced security protocols, conducting frequent audits for data integrity and compliance with security standards.	Implement highly secure offsite storage with limited, authorized access, conducting frequent integrity checks, comprehensive security audits, and detailed access logs.	Opt for top-tier secure offsite facilities with military-grade security measures, biometric and multi-factor authentication for access, conducting frequent integrity and security audits, along with strict access control protocols.
Archiving Duration And Review	Adhere to standard retention periods as per organizational policy, conducting annual reviews for data relevance and legal compliance.	Extend retention periods, conducting semi-annual reviews for data relevance and legal compliance, documenting the review process and outcomes.	Follow specific retention periods dictated by internal policies, conducting regular reviews for data accuracy, relevance, and compliance with internal standards.	Extend retention periods for confidential data, conducting frequent reviews for compliance, relevance, and legal obligations, maintaining detailed logs of review processes and access.	Enforce strict retention guidelines with ongoing review processes, continuously monitor data security, relevance, and compliance, adhering to the highest standards of data protection.

Destruction Table

Activity	Level 1 [Public]	Level 2 [Limited]	Level 3 [Internal]	Level 4 [Confidential]	Level 5 [Top Secret]
Digital File Deletion	Simple deletion using OS commands, with no special logging or verification processes.	Secure deletion employing 3-pass overwriting protocols like the Gutmann method, including log entries with date, time, and user ID.	Advanced cryptographic wiping using tools compliant with FIPS 140-2 standards, with logs containing detailed file metadata, user ID, and verification of successful deletion.	Deletion exceeding DoD 5220.22-M standards, involving 7-pass overwriting, and a comprehensive audit trail including pre-deletion file status, method, operator credentials, and post-deletion verification. Regular integrity audits of deletion tools.	Deletion using custom-developed software with capabilities like variable overwriting patterns, exceeding NSA standards for data destruction. Real-time audit logging with GPS timestamps, operator biometric verification, and post-deletion forensic analysis to ensure irrecoverability.
Physical Media Destruction	Basic physical destruction methods such as snapping discs or hammering USB drives, followed by disposal in general waste.	Degaussing followed by shredding using a P-4 level cross-cut shredder, with destruction logs including media type, serial number, and method.	High-grade degaussing followed by pulverization, with video-recorded destruction processes and logs detailing media type, serial number, degaussing intensity, and pulverization method.	Degaussing with NSA-listed equipment, followed by disintegration into particles smaller than 2mm, and detailed destruction certificates including media type, serial number, degaussing details, and disintegration specifics.	Destruction in a Sensitive Compartmented Information Facility (SCIF) environment using custom-built disintegrators, with end-to-end chain-of-custody documentation from handover to destruction, including video evidence, operator clearance levels, and destruction method details.

Paper Document Shredding	Use of office strip-cut shredders, with shredding performed by general staff without special record-keeping.	Cross-cut shredding reducing documents to 4x40mm particles, with shredding logs including date, time, and responsible staff ID.	Micro-cut shredding to particles not exceeding 2x15mm, following P-5 security standards, performed in controlled areas with access logs and CCTV surveillance.	Use of P-6 level micro-cut shredders, reducing documents to particles under 1x5mm, supervised by security personnel, with detailed logs including document type, volume, and shredding operator details. Frequent audits of shredding processes and machines.	P-7 level high-security shredding in a secured facility, with shredding process including biometric authentication of operators, real-time monitoring, and post-shredding residue analysis. Comprehensive logs with detailed documentation of each document type, quantity, and destruction verification.
Decommissioning Hardware	Standard factory reset followed by environmentally responsible e-waste recycling, with no specific documentation for data wiping.	Data wipe using software compliant with NIST SP 800-88 guidelines, with decommissioning logs including device type, serial number, and wipe verification report.	Decommissioning involving secure wipe protocols, physical disassembly, and destruction of storage components, with comprehensive logs containing device details, data wiping methods, and destruction processes.	Multi-phase decommissioning involving secure data wipe, physical dismantling, and destruction of storage components in a secure facility, with detailed logs including device specifications, wiping method, disassembly process, and final disposition. Regular audits of decommissioning procedures.	Decommissioning in a high-security environment, with data wiping using custom methods, followed by complete physical destruction of components. Full audit trail including device specs, wiping verification, destruction method, and operator clearance levels. Independent validation of data wipe and destruction.

Archived Data Destruction	Routine deletion procedures from archival systems, with no additional measures for data verification post-deletion.	Secure deletion with overwriting protocols, with post-deletion verification checks and logs detailing file metadata, deletion method, and verification results.	Cryptographic erasure from archival systems, following NIST guidelines, with detailed logs including pre-deletion file status, erasure method, and post-deletion integrity check results.	Multi-step deletion process involving both logical and physical data destruction methods, with comprehensive audit logs including file metadata, deletion protocols, operator details, and post-deletion verification. Regular integrity audits of archival systems.	Highly controlled deletion process in a secure environment, with custom-developed erasure software, followed by physical destruction of archived data.