**Name: Farhan Dahir Ahmed**

**Institution: Herzing College**

**Program: Cybersecurity Specialist**

**Data Handling & Storage Procedures**

Data handling and storage procedures are essential for maintaining the confidentiality, integrity, and availability of information. Bellow are some key considerations and best practices for data handling and storage procedures:

1. **Determine How Much Protection Your Information Needs**:
   * Assess the need for confidentiality and the critical nature of the information. Different types of data require varying levels of protection.
   * Classification is crucial here. Information is typically classified as level I, II, or III based on its sensitivity and importance. For insurance:
     + **Level I**: Highly sensitive data (e.g., personal health records, financial data).
     + **Level II**: Moderately sensitive data (e.g., student records, research data).
     + **Level III**: Less sensitive data (e.g., publicly available information).
2. **Collect Only What Is Necessary**:
   * Avoid unnecessary data collection. Collect only the information required for your specific purpose.
   * Minimize the risk of exposure by limiting the scope of data you handle.
3. **Provide Minimum Necessary Access**:
   * Grant access to data on a need-to-know basis. Not everyone needs access to all information.
   * Implement role-based access controls to restrict unauthorized access.
4. **Disclose Only the Minimum Information Necessary**:
   * When sharing data, disclose only what is essential. Avoid oversharing.
   * Be cautious when communicating sensitive information via email or other channels.
5. **Safeguard Information in Transit**:
   * Encrypt data during transmission (e.g., using HTTPS for web traffic).
   * Use secure protocols for file transfers (e.g., SFTP).
6. **Secure Physical Equipment and Resources**:
   * Lock physical servers, computers, and storage devices.
   * Control access to data centers and server rooms.
7. **Safeguard Information in Storage**:
   * Encrypt data at rest (e.g., using full-disk encryption).
   * Regularly back up critical data to prevent loss.
8. **Dispose of Information Securely When No Longer Needed**:
   * Follow proper disposal procedures for physical and digital data.
   * Shred paper documents containing sensitive information.
   * Wipe or securely erase data from storage devices before disposal.
9. **Stay Informed About Information Risks**:
   * Keep up to date with security best practices and emerging threats.
   * Regularly review and update your data handling procedures.

Remember that these guidelines apply to various contexts, whether you’re a university employee, a business professional, or anyone handling data.