12 STEPS TO PROTECTING SENSITIVE DATA IN UNSTRUCTURED FILES GUIDEBOOK

Protecting sensitive data in unstructured files requires a combination of technical measures, policies, and practices. Here are some best practices to consider:

1. **Data Classification:** Start by identifying and classifying sensitive data within unstructured files. Sensitive data includes personally identifiable information (PII), financial data, intellectual property, or any other information critical to your organization.
   - Prioritize your remediation by focusing of the most critical elements first like SSN, credit card number, or clear text passwords.
   - Consider whether sharing sensitive data would be more appropriately stored in databases on servers.

2. **Access Control:** Limit access to sensitive files to only those who need it for their job responsibilities. Implement role-based access control (RBAC) and enforce the principle of least privilege, ensuring that users have only the permissions necessary to perform their tasks.
   - For OneDrive, right-click on a shared folder or file, navigate to OneDrive and then select Manage access. (NOTE: OneDrive sharing is not available for external parties.)
   - For SharePoint, go to the list, library, or survey and open it.
     i. Go to the Permissions page using the steps in the previous section.
     ii. Select Grant Permissions on the Permissions tab.

3. **Encryption:** Encrypt sensitive data both at rest and in transit with cryptography commensurate with the sensitivity of the data and keep it current. Utilize strong encryption algorithms to protect the content of the files from unauthorized access so even if files are compromised, the data within remains unreadable.
   - For Microsoft Office files, click on the **File** tab.
     - Select **Info** from the left sidebar.
     - Under the Protect Workbook section, choose **Encrypt with Password**.
     - Enter a password of your choice and click OK and re-entering to confirm.
   - Store your agency's passwords in Azure Key Vault (for admins) or a password manager.
   - Alternatively, subscribe to VITA's "File Level Encryption" service

4. **Data Loss Prevention (DLP):** Implement DLP solutions to monitor and control the movement of sensitive data within and outside the organization. DLP tools can help detect and prevent unauthorized access or transmission of sensitive information.
   - Submit an RFS for a data loss prevention solution

5. **Data Masking and Anonymization**: Mask or anonymize sensitive data when it's not needed for processing or analysis. Replace actual data with realistic but fictional data to protect privacy while still maintaining usability for certain purposes.
   - Excel Masking - How to Hide Confidential Data in Excel (5 Easy Ways) - ExcelDemy
   - Excel Anonymization - Anonymize Data in Excel

Contact ODGA's Data Protection and Governance Team for assistance.

6. **Audit Trails and Logging:** Maintain detailed audit trails and logging mechanisms to track access to sensitive files. It's important to monitor who accessed the files, what changes were made, and when they occurred, facilitating accountability and incident investigation.
    - If the file is shared in Teams or SharePoint, click on the filename in the upper left-hand corner while the file is open. Click on **Version History** to view changes or restore a prior version
    - Partner with VITA to review system logs if there are security concerns.

7. **Regular Audits and Assessments:** Conduct periodic audits and security assessments of your file storage systems to identify vulnerabilities and ensure compliance with security policies and regulations.
    - Teams Channel and SharePoint owners should periodically review file sharing and permissions

8. **User Education and Awareness:** Educate users about the importance of safeguarding sensitive data and provide training on security best practices. Encourage employees to use strong passwords, avoid sharing credentials, and report any suspicious activities promptly.
    - Ensure all required Sec 527 training is complete including any agency-specific regulatory training such as FTI, SSA, or PCI) using VITA's KnowBe4 platform or similar products.

9. **Secure File Transfer Protocols:** Use secure file transfer protocols such as SFTP (SSH File Transfer Protocol) or HTTPS when transmitting sensitive files over networks. Avoid using unencrypted protocols like FTP.
    - To securely share sensitive information with external parties, use the Virtru or Box service from VITA

10. **Data Retention and Disposal**: Establish policies for the secure retention and disposal of sensitive files. Regularly review and securely delete files that are no longer needed to reduce the risk of unauthorized access or data breaches.
    - Please review the retention schedules for state agencies at the Library of Virginia Records Management - Retention Schedules (virginia.gov)
    - Sec 514 - Instructions for Removal of COV Data

11. **Endpoint Security**: Implement endpoint security measures to protect devices that access or store sensitive files, including antivirus software, endpoint detection and response (EDR) solutions, and device encryption.
    - VITA provides several tools for endpoint security protection such as CrowdStrike and BitLocker.

12. **File Integrity Monitoring:** Deploy file integrity monitoring solutions to detect unauthorized modifications or access to sensitive files to help in detecting and responding to security incidents in a timely manner.
    - Purchase a tool such as Tripwire, Netwrix, or Microsoft Defender for Cloud's File Integrity Monitor

If you suspect any possible data breach, follow your security incident response protocol and notify your ISO. If there's a confirmed issue, report it to the VCCC. By implementing these best practices, organizations can better protect sensitive data within unstructured files and mitigate the risk of data breaches or unauthorized access.

Contact ODGA's Data Protection and Governance Team for assistance.