Subject: **Cyber Security Advisory - Securing Sensitive Digital Documents and Confidential Files (Advisory No. 22)**

Context. NTISB has been issuing advisories related to Information Security from time to time to safeguard confidential information from unauthorized access. Due to the increasing frequency of unauthorized access incidents affecting a variety of organizations in Pakistan, including government agencies, private institutions, and public service sectors, NTISB has identified increase in incidents involving unauthorized access associated with the handling, storage, and transfer of sensitive digital documents and confidential files. The unauthorized exposure of sensitive information, whether through malicious intent or accidental mishandling, can severely compromise organizational integrity, data confidentiality, and the National Security. Aim of the advisory is to reiterate and provide guidelines for the secure management of sensitive files in digital formats, including scanned documents, soft copies, and internal records, to minimize the risk of unauthorized access and potential breaches.

2. **Impact**. The compromise of sensitive digital documents and confidential files can result in severe consequences, including unauthorized access to internal records, exposure of confidential data, breach of organizational and governmental trust, and potential threats to national security. Addressing vulnerabilities in information handling and access control is therefore essential to mitigating these risks and maintaining data integrity.

3. Affected Systems and Entities. Entities handling sensitive documents in digital form, particularly those using networked systems, cloud storage, or external storage devices for file management, are at increased risk of unauthorized access. This includes government agencies, public institutions, private organizations, educational institutions, and SMEs that store or transmit sensitive information.

4. Recommendations & Action Items. NTISB recommends the following measures to secure digital files and prevent unauthorized access to confidential records:

a. **Implement Strong Access Controls**. Use role-based access control (RBAC) to limit access to sensitive files strictly to authorized personnel. Assign permissions based on job roles, ensuring that only those with a legitimate need have access to confidential information.

b. **Enforce Multi-Factor Authentication (MFA) for Sensitive Files Access.** Require multi-factor authentication (MFA) for accessing files containing sensitive information, especially for administrative and privileged accounts. Implement authentication mechanisms such as hardware tokens, mobile-based verification, or biometric authentication to add an additional layer of security as deemed appropriate.

c. **Encrypt Sensitive Digital Files**. Utilize robust encryption algorithms for storing sensitive files, both on local servers and cloud-based storage. Encryption ensures that even if files are accessed by unauthorized users, the content remains protected.

d. **Use Secure File Transfer Protocols**. When transferring sensitive files digitally, use secure file transfer protocols, such as SFTP or HTTPS, to protect data in transit from being intercepted or tampered with.

e. **Implement Document Watermarking.** Apply digital watermarks to sensitive files to identify document owners and trace unauthorized distribution. Watermarking provides an added layer of traceability and deterrence against unauthorized sharing of documents.

f. **Audit Access Logs Regularly**. Enable logging for all access to sensitive files, with regular audits to monitor unusual or unauthorized access attempts. Maintain audit trails for an adequate retention period to support any necessary investigations.

g. **Educate Employees on Information Handling Best Practices**. Conduct training sessions and awareness programs for employees to reinforce best practices for handling sensitive information. Employees should be aware of potential risks and understand secure data management procedures.

h. **Implement Data Loss Prevention (DLP) Systems**. Deploy Data Loss Prevention (DLP) systems to monitor and control the sharing of sensitive information within and outside the organization. DLP systems can detect and prevent unauthorized sharing or movement of confidential files.

i. **Control External Device Access.** Limit or restrict the use of external storage devices (e.g., USB drives) for storing or transferring

sensitive information. Implement policies for device encryption and track device usage to prevent data exfiltration via physical media.

j. **Conduct Regular Vulnerability Assessments and Penetration Testing.** Perform periodic vulnerability assessments and penetration testing on systems managing sensitive documents. These tests can help identify and address potential security gaps that could lead to unauthorized access.

k. **Create and Enforce a Strong Password Policy**. Mandate complex passwords for systems accessing sensitive files, with policies that include minimum length requirements, a combination of alphanumeric and special characters, and regular password updates.