To: All Staff Members

From: [Security/Risk Management Department]

Date: [Insert Date]

Subject: Internal Advisory: Insider Threat Mitigation and Data Security

Dear Team,

As a financial institution, the protection of our clients' assets and sensitive data is our highest priority. To maintain the integrity of our operations, this advisory serves as a reminder of our collective responsibility to mitigate internal risks.

Key Indicators of Insider Threats:

- Unauthorized attempts to access sensitive financial data or systems.
- Frequent, unexplained downloading or exporting of large datasets.
- Bypassing standard security protocols or using unauthorized software.
- Working irregular hours or accessing the office at unusual times without justification.

Mandatory Security Practices:

- Never share your system credentials, passwords, or MFA tokens with anyone.
- Ensure all physical documents containing Client Identifiable Information (CII) are shredded when no longer needed.
- Report any suspicious activity or requests for sensitive information to the [Security Office/Whistleblower Hotline] immediately.
- Log out of or lock your workstation every time you leave your desk.

Reporting Channels:

If you observe behavior that compromises our security standards, please use the following confidential channels:

- Email: [Internal Security Email Address]
- Hotline: [Internal Extension or Phone Number]
- Portal: [Link to Anonymous Reporting Tool]

Compliance with these guidelines is mandatory. Failure to adhere to security policies may result in disciplinary action, up to and including termination and legal proceedings.

Thank you for your commitment to keeping our institution secure.

Regards,

[Name/Signature]
[Title]
[Department Name]