BTP Security Matters Checklist

There are procedures and practices necessary to make any business truly secure.

BTP protects its clients in the following ways:

All systems require two or more authentication methods for access

To access email or any other system, users must 1) provide an ID and password and 2) authenticate in a second way via phone confirmation, a security fob, or biometric identification. This prevents access in the event an unauthorized party discovers a user's ID and password, which is the most common way security is compromised.

System access is immediately terminated for ex-employees, contractors, and vendors

A termination checklist is used to make sure access is cut off for those no longer connected to your firm. Audit records are kept comparing termination notice times to access termination times.

Systems are subject to regular third-party security audits

All prior audit reports are preserved, and results are noted in management committee meeting minutes every three months.

External and internal penetration tests are conducted by unaffiliated third parties

Internal penetration tests are performed to calculate the risks in employee and contractor system access. These tests are performed by objective external organizations with no other financial relationship with the firm or its information technology vendors.

There is a written security policy that can be shared with clients

The policy includes a requirement for management review and for keeping the policy up to date with changing technology and threats.

A secure inventory of sensitive data is maintained

There is a person responsible for knowing the nature of your data, its security sensitivity, and how it is protected, stored, and backed up. Procedures are in place to ensure that all data received, generated, or transmitted is inventoried, evaluated, and protected appropriately.

Anyone with access to internal systems receives periodic security education

Employees receive security training every six months and are assessed to confirm the material has been learned. They receive continuing education credit for these trainings.

Password rules are systematically enforced

All passwords are stored in a password management system. Passwords are required to have strong security, are changed at regular intervals, and are never written down or reused.

There are automated means of detecting system attacks

Both automated alerts and human review are used to look for and report on unusual activity such as system intrusions, unauthorized access, system corruption, and unexpected data transfers that could indicate malicious intent.

Sensitive data is not allowed on unmanaged devices

Sensitive data is locked down with strong encryption and kept from unmanaged devices like phones, tablets and laptops. Security is assured for all data, even if some of it resides on a lost device or an ex-employee's "bring your own device".

Anti-virus and anti-malware protection are required on all devices

A centralized monitoring/updating system ensures 1) a complete inventory of devices and installed software, 2) knowledge of versions and patch levels of all this software, 3) continuous management and monitoring of every end point keeps protections and software up to date with the latest, most secure production versions available.

Precautions are in place to prevent third parties from eavesdropping on or viewing sensitive data inside or outside offices

Interior workspaces are configured to prevent unauthorized screen viewing or the overhearing of sensitive information. Everyone who works with sensitive data outside the offices are required to use physical security screens on portable devices or limit their use to secure spaces.

Backups of all critical data are periodically tested

Backups are made regularly so systems can be restored at any time. Documented procedures are followed, and the time taken to restore is recorded.

Backups are systematically protected against ransomware corruption

Backups are maintained both offsite and offline. Full copies of all system and application software are kept on read-only physical media. Software backups are confirmed to be 100% identical to the read-only master copies of all software.

Anti-phishing tests are frequently and randomly performed

The best defense against phishing, a common and very successful hacking technique in which authorized users are tricked into entering or otherwise revealing their user ID and password, is to create awareness through random tests of all users by independent auditors.

Sensitive data is protected through physical security measures

Offices and records are secured with locks, entry/exit logs, cameras, and alarms. Employees are trained and required to physically secure data and to report security breaches or risks.