Information Technology Health & Security Checklist

InfoSight Inc suggests the following technology, policies and procedures for optimal data security and system performance. We offer a wide range of professional services that include performing any or all of these recommendations, and more. Visit our website at www.InfoSightInc.com for a complete explanation of security-related products and services.

☑ TECHNOLOGY CHECKLIST

- ☐ Firewall is installed and regularly updated.
- ☐ Intrusion Prevention technology is used to prevent unauthorized access to system resources.
- ☐ Anti-virus and Anti-malware software is installed and updated regularly.
- ☐ Anti-spyware technology is installed and updated regularly.
- ☐ A patch management program is used to patch and regularly update operating systems, software and web browsers.
- ☐ Server Event Log Monitoring is enabled and logs are reviewed regularly.
- ☐ An Email Content Filtering solution is used to prevent the loss of sensitive information and to filter out spam, viruses, computer worms, denial-of-service attacks, Trojans, spyware, etc.
- ☐ Endpoints are secured (i.e. USB ports, blue-tooth, flash drives, etc.)
- ☐ Encryption technology is used on email, portable storage and mobile devices.
- ☐ An Email Archival solution is used to reduce email server load, and provide quick access for response to litigation.
- ☐ Critical files are routinely backed up and are periodically archived offsite.
- ☐ Internet Content Management tools are used to screen undesirable Web pages and prevent data loss via webmail and/or social networks.
- ☐ Privacy and security settings in software, browsers, email programs, and online accounts including social media are evaluated regularly.
- ☐ Group policies have been created in Active Directory to limit users rights to data.
- ☐ An Independent IT Security Posture Review is performed periodically.
- ☐ Online banking customers should perform a Risk Assessment and Controls Evaluation periodically.

☑ POLICY CHECKLIST

- ☐ Information Security Awareness Policy
- ☐ Privacy Policy
- ☐ Acceptable-Use Policies
  - Workstation
  - Internet
  - Email
  - Mobile Device and Wireless
- ☐ Remote Access Policy

- ☐ Social Media Policy
- ☐ Business Continuity/Disaster Recovery Policy

☑ USER CONDUCT CHECKLIST

- ☐ Has participated in Information Security Awareness Training.
- ☐ Uses strong passwords with a minimum of eight characters and a combination of numbers, upper-case letters, lower-case letters and symbols.
- ☐ Forces password changes at least every 60 days.
- ☐ Doesn't share their User IDs and Passwords with others.
- ☐ Never clicks the box to "remember" passwords.
- ☐ Uses Windows Task Manager (Control+Alt+Delete) to close any pop-up dialog boxes, rather than selecting "no" or "cancel" or the "X" icon in the title bar.
- ☐ Deletes all cookies and history when closing your Web browser.
- ☐ Doesn't save important financial links in their favorites & bookmarks.
- ☐ Never opens unknown email messages or attachments.
- ☐ Doesn't use webmail, IM chat, music/video streaming and/or social networking on the corporate network.
- ☐ Notifies the bank when personnel using online services have changed.
- ☐ Reports to the bank any online activity relating to banking that seems suspicious.
- ☐ Doesn't blindly accept a disc or flash drive without scanning it first with security software.
- ☐ Doesn't download apps to the corporate network.
- ☐ Doesn't download application plug-ins to the corporate network.

ABOUT US: InfoSight, Inc. offers proven, affordable Managed Security, IT Compliance and Vulnerability services that protect and optimize how an organization's critical information is processed, managed and stored. For more than 10 years, InfoSight has served organizations nationwide minimizing risk exposure and providing the highest levels of security assurance and IT regulatory compliance. InfoSight services combine consulting with technology including Perimeter Security & Infrastructure Monitoring Services, Email and Internet Content Services, Data Leakage & Data Privacy/ Policy Enforcement Services, IT Risk Assessment & Compliance Consulting, and Enterprise Network Implementation Solutions.