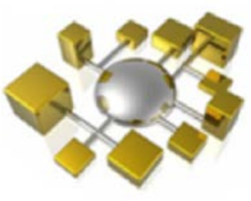

LSS_Audit

AccueXchange USB Policy Audit Plan

Duy Nguyen Jason Mays

Vince Kelly Pascal Allison

Table of Contents

Executive Summary

To AccueXchange Executive Management,

Thank you for taking the initiative to improve your business policies and processes by allowing us to audit AccueXchange's acceptable mobile devices and removable media use policy.

Lock Tight Security Services is committed to IT security and understands the importance of cybersecurity to an organization. By allowing LSS to review the removable device policy**,** you've ensured minimal impact to business operations in event of exploited data and/or internal operations. Additionally, AccueXchange will be able to reduce the complexity of assessing a security baseline, identifying/prioritizing risks, and establishing effective cybersecurity measures in reference to removable devices usage. Based on our Risk Matrix of AccueXchange policies, the organization will be able to decide to either accept, transfer, and or mitigate these identified risks.

Based on LSS's review of AccueXchange e's removable devices acceptable use policy, we have identified the below high-level risks:

- Policy compliance and awareness
- Restriction of non-approved removable media devices use on Organizational infrastructure
- Restriction on removal of approved media removable from Organizational facilities
- Failure to report police's noncompliance

Further discussion of Ace's findings is welcomed, we can be scheduled for review of findings or recommendations based on findings at LockSecurityServices@gmail.com.

Lock Tight Security Services,

Objectives

There are two overall objectives for this Audit. The first is to perform a comprehensive evaluation of AccueXchange's existing policies regarding the Use of USB Drives and Removable Media. This includes identifying existing controls and associated risks so that AccueXchange internal organizations can make effective risk decisions based on our findings. After establishing an audit baseline from the first objective, the second objective will be to leave AccueXchange with a completely automated USB monitoring and enforcement mechanism, the section on Audit Strategy in this document expands upon this and provides more detail)

Audit Strategies

LSS will provide a unique approach to the AccueXchange audit strategy in that, in addition to the administrative and physical controls that have already been established as part of the original USB security policy, LSS will establish an additional set of technical controls that will enable AccueXchange to completely automate both its USB policy monitoring and its USB enforcement processes. LSS has developed a comprehensive, multi-level, automated system for the detection, identification, reporting, and prevention of unauthorized access or use of USB devices anywhere within an AccueXchange facility. This system comes in three variations:

- Basic USB Monitoring and Enforcement system called 'usbSniffer". This is a basic, platform-independent software offering that can be applied to a single device on the AccueXchange premises.
- Advanced USB Monitoring and Enforcement system. Extends the capabilities of the Basic usbSniffer software platform to provide centralized monitoring and enforcement of all usbSniffer instances across the entire AccueXchange enterprise.
- In addition, (for a separate monthly subscription fee), LSS can provide an opportunity for AccueXchange to take advantage of its managed security service offering called "Advanced Plus USB monitoring Service". This service centralizes USB policy management within the LSS Security Operations Center (SOC) and adds multi-user, roles-based access control features to the Advanced USB monitoring and enforcement system. This ensures a complete separation of duties is observed for the management, control, and operation of the system.

Two videos have been provided that describe these offerings in more detail:

- An information and background video that provides specific answers to the questions that AccueXchange posted as part of the RFI that it recently published. This video describes the purpose of the strategy and a high-level overview of how the system works.
- A video that provides a demonstration of the Basic and Advanced USE Monitoring and Enforcement software.

Audit Plan

Removable media devices are very innocuous and convenient for AccueXchange, but with the convenience come risks. A risk analysis was performed which brought live an overwhelming result. The analysis identified lots of risks associated with USB usage that has the potential to cause problems for organizations which AccueXchange, is no exception.

By reviewing AccueXchange, operations, and activities, the Removable media devices use policy is formulated with specific goals, controls, and evidence for success.

The policy set controls for USB usage and practices. These controls will mitigate or reduce the risks.

The policy creates the allowance for continuous check and balances for goals achievement, controls, and evidence of policy adherence or violation.

To better understand the background of AccueXchange,'s Policy please refer to attached video the LSS team has created. Please view attached video *AccueXchange_Background.*

Conclusion

Lock Tight Security Services is committed to providing AccueXchange with first-class auditing services. Our dedicated an experienced team will work with AccueXchange to mitigate security risk through:

- Active employee security engagement training
- Employing practical systems and processes into seamlessly into AccueXchange, workflows
- Maintaining policy compliance with AccueXchange 's risk appetite and remain within AccueXchange, risk tolerance

We look forward to providing auditing services at the highest level of quality you can only expect from Accu-Audit.

Engagement Team

Name	Title
Duy Nguyen	CEO
Vince Kelly	Audit Account Director
Pascal Allison	Audit Engagement Director
Jason Mays	Audit Engagement Lead

Policy Goals – Risks Matrix

Policy Goals	Controls	Risks	Evidence
Acceptable Use	USB drives are not to be left unattended	• Possible loss of PII, sensitive data, and/or Organization's intellectual property at risk • Unauthorized users accessing organizational data • Policy insufficient • Training insufficient • Employee non-compliant • Employee unaware of reporting process	• AccuExchange USB – Use Policy • AccuExchange USB – Use Video
Acceptable Use	USB drives are not removed from the facilities	• Possible loss of PII, sensitive data, and/or Organization's intellectual property at risk • Unauthorized users accessing organizational data • Policy insufficient • Training insufficient • Employee non-compliant • Employee unaware of reporting process	• AccuExchange USB – Use Policy • AccuExchange USB – Use Video
Acceptable Use	No other removable media outside of USB devices are being used	• Non-approved devices may contain damaging malware/viruses that may endanger organizational information and information systems • Policy insufficient • Training insufficient • Employee non-compliant • Employee unaware of reporting process	• AccuExchange USB – Use Policy • AccuExchange USB – Use Video • USB Sniffer Tool Logs

Acceptable Use	Spot checks to ensure compliance and that drives contain appropriate content to the best of their ability	• Possible loss of PII, sensitive data, and/or Organization's intellectual property at risk • Policy insufficient • Training insufficient • Employee non-compliant • Employee unaware of reporting process • Employee unaware of reporting process	• AccuExchange USB – Use Policy • AccuExchange USB – Use Video • USB Sniffer Tool Logs
Acceptable Use	Training	• Less satisfied employee • Low productivity • Inappropriate action	• AccuExchange USB – HR Policy • AccuExchange USB Incident – Meeting • Communicate all action taken for violation
Acceptable Use	Monitoring	• Non-compliance	• Records of case on file • AccuExchange USB – logs • Compliance
Acceptable Use	Policy mandates individuals must not use USB drives for anything other than appropriate and proper AccuExchange business activities	• Slow adoption of authorized USB resulting in loss of productivity • Policy violation/ Increased employee reprimands	• AccuExchange USB – Responsibilities Policy • Training • AccuExchange USB – Use Policy • AccuExchange USB – Use Video
Acceptable Use	Unapproved USB drives or encryption software from any non-AccuExchange individual or company is not permitted	• Policy violation/ Increased employee reprimands • Less satisfied employee • Slow adoption of authorized USB resulting in loss of productivity	• AccuExchange USB – Responsibilities Policy • Training • AccuExchange USB – Use Policy • AccuExchange USB – Use Video

Acceptable Use	Restriction of employee executable code or automatic command execution files on AccuExchange USB drives.	• Slow adoption of authorized USB resulting in loss of productivity • Policy violation	• USB sniffer logs
Acceptable Use	Policy mandates USB labels and volume serial numbers may not be tampered with or removed	• Slow adoption of authorized USB resulting in loss of productivity • Policy violation • Policy violation/ Increased employee reprimands	• AccuExchange USB-OA Records
Non-Acceptable Use	Meeting with HR and Manager	• Inappropriate reprimands • Legal issues • Policy violation	• AccuExchange USB – termination policy • Employee files • Legal proceeding records • Document all inadequate termination, save on employee file
Incident Management	Tracking and audit logs are being maintained and that all physical, technical and administrative controls are in place and being followed	• Policy insufficient • Training insufficient • Employee non-compliant • Employee unaware of reporting process • Employee unaware of reporting process	• AccuExchange USB – Use Policy • AccuExchange USB – Use Video
Incident Management	Quarterly reports to the CIO of all USB activities with particular attention paid to lost devices (the loss circumstances, what information was on the drives, the frequency of losses, etc.)	• Policy insufficient • Training insufficient • Employee non-compliant • Employee unaware of reporting process • Employee unaware of reporting process • Incident process insufficient/ineffective	• AccuExchange USB – Use Policy • AccuExchange USB – Use Video
Prevention of data loss	The restricted use of non-AccuExchange removable media	• Loss of productivity due to lack of access to an authorized USB • Policy violation/ Increased employee reprimands • Less satisfied employee	• AccuExchange USB – Responsibilities Policy • Training • AccuExchange USB – Use Policy

			• AccuExchange USB – Use Video
Prevention of data loss	WinEncrypt USB drive with CryptArchiver encryption	• Slow adoption of authorized USB resulting in loss of productivity • Bottleneck effect caused by maintenance	• Flash drive data recovery and initialization logs • AccuExchange USB-OA Records • USB sniffer logs
Implement role-based access	OA is the only personnel permitted to reformat USB drives.	• Loss of productivity due to inability of use of authorized USB during maintenance • Policy violation/ Increased employee reprimands • Bottleneck effect caused by maintenance	• Flash drive data recovery and initialization logs • USB sniffer logs
Prevention of data loss	Policy mandates restriction of specific categories of information being stored on any AccuExchange USB drive: • Copyrighted material of any kind • Company proprietary or non-company proprietary information of any kind. • Illegally obtained source or executable software, files, data or content of any kind. • Music, pictures, recordings, videos or any information of a personal nature • USB thumb drives are not permitted to be used as storage devices for any file sharing, peer-to-peer or bit torrent content of any kind. • Downloading and storing files from the Internet	• Policy violation/ Increased employee reprimands • Slow adoption of authorized USB resulting in loss of productivity • Less satisfied employee	• AccuExchange USB – Responsibilities Policy • Training • AccuExchange USB – Use Policy • AccuExchange USB – Use Video • USB sniffer logs • AccuExchange USB-OA Records