Security Policies and Procedures

Process Owner: Rob Fea
Created: 6/23/2016
Last Update: 01/29/2018
Last Update By: Rob Fea

Summary

Our customers trust us with access to their systems and in many cases access to documents and files that contain sensitive data. To preserve this trust and protect the identities of people referenced in those files, it is critical that we take every measure possible to protect access to our buildings, servers, email, and other possible windows into this sensitive information.

This document and all referenced documents can be found here: ***I:\Common\@All Company\Security***

Who is responsible for security at Extract?

You are! Security should be at the forefront of your mind during all interactions with customer's and our systems.

Who should you contact?

Rob Fea is the current owner of all security policies and processes. Reach out to him with any questions, concerns, or ideas for improvement. Please also include on those communications any other relevant parties here at Extract.

Background Checks

Prior to employment, every employee must pass a Criminal Background check that is performed by Sterling Infosystems, Inc. This is to ensure that our employees don't have anything significant in their history that would prevent them from handling customer information in a responsible way.

Office Access

Access to our office is restricted to employees via the use of access fobs or entry cards. These fobs are issued upon employment and are immediately deactivated upon employment termination. All entries and exits from the office are logged and can be reviewed by a system administrator.

Server Access

Access to the server room is restricted to a subset of five tenured employees via the use of access fobs. These fobs are immediately deactivated upon employment termination. All entries and exits from the server room are logged and can be reviewed by a system administrator. Any access by an employee without explicit server access MUST be chaperoned by a user with access.

Security System

Extract's offices are protected via an ADT security system. Only full-time employees are given the passcode and the passcode is changed whenever an employee's relationship with Extract ends.

Regularly Scheduled Network and Security Audits

Extract has contracted an outside vendor to perform regularly scheduled network and security audits (approximately once per year). Upon completion of these audits any known weaknesses are addressed in a timely manner.

In addition, Extract's security team performs an internal network and security audit bi-annually. The most recent and all historical audits can be found here: ***I:\Common\@All Company\Security\Audits***

Installation of Software on Extract Machines

All software that is installed on local machines must be approved by the Extract IT team prior to installation. Do not simply click through license agreements assuming they have no implications to us or our customers. Certain types of software are strictly forbidden, including applications such as BitTorrent and Tor.

Security Breach Process

Please refer to the document **Extract - Data Breach Response Policy.pdf** for a full explanation of Extract's data breach policies and procedures.

External Access by Vendors and Subcontractors

Vendors and subcontractors are held to the very same standards as our employees. Each vendor or subcontractor who accesses any of our systems is required to sign a BAA (see **Extract - Master BAA (PHI).doc**) in which they must agree to our data sharing policies.

HIPAA, PHI, PII and Other Sensitive Data

Extract has several measures in place to ensure that employees and customers always treat Protected Health Information (PHI) and Personally Identifiable Information (PII) with extreme caution:

1. The primary way to avoid data breaches or misuse of sensitive data is to avoid having it at all. The vast majority of sensitive data resides on the customer's servers.
2. Sensitive sample documents that are required for our rule-writing efforts, internal service projects, or troubleshooting are stored on a secure NAS device that is encrypted at rest. Permission is restricted to only those requiring access for the project. The NAS device is a Synology RS3617xs+, which has a Hardware Encryption Engine (AES-NI). You can view the hardware specs here. Each customer has their own encrypted share on this device with a 25-character key with upper-case, lower-case, and numbers. This key is only accessible by a system admin and is destroyed along with the files upon deletion.
3. When sensitive must be transmitted between a customer site and Extract, it is done in one of these ways:
    a. Encrypted files using AES-128 encryption or higher.
    b. Secure FTP using SSL or SSH.
    c. Site-to-site VPN.

All employees much watch the following training videos as part of their employment with Extract:

- What is HIPAA?
- What is PHI?

And in case the worst case does occur, Extract has a formally documented data breach response policy: **Extract - Data Breach Response Policy.pdf**.

Employee Awareness

All Extract employees must review and sign this document upon being hired at Extract. This policy is reviewed regularly at all-company meetings and specific pieces of it are discussed in detail to ensure that employees are current on the policy and any changes to it.

Employee System Access

Employees are given access to internal servers, directories, and systems as well as customer systems based on their role and the appropriateness of that access. All Extract employees are required to have a unique user IDs and passwords. Access to customer systems is NEVER granted without customer consent and employees only access customer networks using customer-approved secure remote access methods.

Upon termination of employment, all physical and electronic access to the office and all of Extract's systems is revoked.

System access group policies enforce an automatic timeout after 15 minutes of no activity and systems will be locked down after 10 failed login attempts. Network passwords expire and must be re-set every 60 days. Passwords must:

- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- Be at least eight characters in length
- Contain characters from three of the following four categories:
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Base 10 digits (0 through 9)
    - Non-alphabetic characters (for example, !, $, #, %)
- Have not been used as one of the user's previous four passwords
- Have not been changed in the last two days

Complexity requirements are enforced when passwords are changed or created.

See Office Access and Server Access sections above for details on physical access by employees.

Removable Media

No removable media devices, including phones, should be connected to Extract machines without explicit permission from the Extract security team.

Firewall

Extract currently has a dedicated business-class firewall to protect our network from outside intrusion attempts.

System Maintenance

Extract maintains all of its servers to be sure they are up-to-date with the latest operating systems and security patches. All servers are assessed every two months and necessary patches and hotfixes are installed as needed.

Endpoint Security Software

Extract currently uses Symantec Endpoint security on all servers and user machines. The software protects against viruses and malware. There is an active scan weekly on all servers and full scan setup for workstations. Email and files downloaded from the internet are scanned.

Policy Change Notification Process

Significant changes to the security policies in this document will be communicated to Extract employees and an updated signature may be required.

Employee Acknowledgment and Signature

By signing below, I acknowledge receipt and understanding of the Extract Systems, LLC Security Policies and Procedures. I also acknowledge that I have watched the training videos that are outlined in the Security Policies and Procedures document.

Employee Name: _____

Employee Signature: _____

Date: _____