ETC Third-Party Vendor Security Policy

Version 1.2

March 17, 2021

Document History

Date	Revision Version	Author	Summary of Changes
May 10, 2016	1.0	ETC	Initial Submittal
October 11, 2017	1.0	Chuck Miller	Annual Review
January 29, 2019	1.0	Austin Moseley	Annual Review
February 19, 2020	1.1	Austin Moseley	2020 Annual Review. Updated for password length
February 18,2021	1.1	Austin Moseley, Thien Pham, Regina Weishuhn, Joel Anjilimoottil, Chrystal Kimbrough, Emanuel Escobar, Najeeb Barney	2021 Review
March 17, 2021	1.2	Thien Pham	Update Company name

Table of Contents

1. Purpose

This policy is designed to protect ETC's non-public information and information resources by listing the required security controls of third-party vendors who will connect to ETC information resources and/or gain access to non-public information.

2. Scope

ETC's third-party vendors are required to implement, test and continually monitor the security controls outlined below to protect ETC sensitive data (including, but not limited to, financial data, credit card information, ETC customer data (including their respective patrons' information) and employee data).

Satisfactory compliance with these security controls is predicated upon the completion of an Information Security Questionnaire conducted by the ETC Information Security Group. Periodic reassessments and onsite audits may be required to ensure continued compliance with the ETC security controls.

3. Security Controls

1) Authentication and Access Control
   a) Vendor must have a formal, documented process for granting and revoking access to all systems that process, store or access ETC sensitive data.
      i) Immediate revocation of network access upon termination.
      ii) Notification mechanism for ETC.
      iii) Yearly review of authorized users.
      iv) Unique user ID which must not be shared with any other individual.
         (1) Delete disabled accounts after 90 days.
         (2) Disable inactive accounts after 30 days.
         (3) Session lock after 15 minutes of inactivity.
            (a) Requires a password or biometric authentication to resume.
      v) Passwords for unique user ID's must meet the following criteria:
         (1) Passwords should be a minimum of 14 characters.
         (2) Implement password complexity to contain at least 3 of the 4 rule sets.
            (a) Passwords should contain at least one upper-case letter.
            (b) Passwords should contain at least one lower-case letter.
            (c) Passwords should contain at least one number.
            (d) Passwords should contain at least one special character (for example, #, $, !, %).
         (3) Password expiration after 90 days or less.
         (4) Lockout after no more than 6 failed attempts.
            (a) Disabled for a minimum of 30 minutes unless unlocked by an administrator.
         (5) Assign randomly generated passwords for new users or password resets.
   b) Vendor must incorporate two-factor authentication for remote network access originating from outside the network by personnel and all third parties.
2) Network Security
   a) Vendor must use IDS and/or IPS techniques to detect and/or prevent intrusions into the network.
      i) Deployed on the perimeter(s) of the network.
      ii) IDS and/or IPS firmware/software/operating system is kept current.
      iii) Current and automated updating of IDS/IPS signatures/definitions.
      iv) Generate audit logs to a centralized location.
      v) Alerting enabled along with evidence/review of such alerts.
   b) Vendor must implement stateful-inspection firewalls.
      i) Deployed at all Internet perimeters.
      ii) Deployed between internal, external, and DMZ zones.
      iii) Quarterly review of firewall rules.
   c) Vendor must segregate between ETC and non-ETC networks.
      i) Firewalls, routers, and/or switches with access-control lists should be used to segregate networks properly.
   d) Vendor must maintain an updated network diagram detailing LAN/WAN segments, firewalls, routers, and switches and provide to ETC upon request.
3) Vulnerability Management
   a) Vendor must have a documented patch management and distribution process that ensures all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches.
      (1) Critical patches should be applied within one month of release.
   b) Vendor/BA must perform yearly internal and external vulnerability testing by a qualified internal resource or external third-party.
   c) Vendor/BA must deploy anti-virus and anti-malware on all systems commonly affected by malicious software.

i) Anti-virus and anti-malware firmware and software are kept current.
ii) Current and automated updating of anti-virus and anti-malware signatures/definitions.
iii) Perform periodic scans (preferred setting is weekly).
iv) Generate audit logs.
v) Ensure anti-virus and anti-malware mechanisms cannot be disabled or altered by users.

d) Vendor must implement personal firewalls on all workstations and/or laptops.
i) Ensure personal firewalls cannot be disabled or altered by users.

4) Media Protection, Sanitization and Destruction
a) All ETC sensitive data stored by vendor will be protected with data-at-rest encryption technology utilizing a 128-bit or higher cryptographic key.
i) Removable media and/or mobile devices will not be used by the vendor to store or transport any ETC sensitive data unless explicitly approved, in writing, by ETC.
b) Upon termination of the contract with ETC or at any time prior to reuse or repurposing of media used to store or process ETC sensitive data, said media must be sanitized using NIST SP 800-88 methods.
i) If the media is to be destroyed, the method used must ensure that after destruction, the media is able to withstand a laboratory attack as outlined in NIST SP 800-88.
ii) Vendor must provide a certificate of destruction if requested by ETC.

5) Security Awareness and Training
a) Vendor must ensure all users receive regular security awareness training.
i) Annual secure coding training (for developers) including OWASP Top 10.
b) Vendor must ensure all designated security personnel and IT management are apprised of the requirements outlined within this agreement.
c) Vendor must designate an individual with oversight responsibilities of the information security program.

6) Auditing
a) Vendor must implement centralized logging for system/network activity.
i) Alerting enabled to notify of critical events.
ii) Minimum of weekly review of log activity.
iii) 1 year retention of logs.
iv) Audit logs must be read-only and protected from unauthorized access.
b) Vendor must employ a regular audit log review process (either manually or automated) for detection of unauthorized access to ETC sensitive data.

7) Data Transmission Confidentiality and Integrity
a) Vendor will use strong encryption, cryptography, and security protocols (for example, TLS, IPSec, SSH, SFTP) to safeguard ETC sensitive data during transmission over open, public networks.

8) Incident Response
a) Vendor will implement incident response plan/procedures and be prepared to respond immediately in the event of unauthorized system and/or network activity.
i) Incident response plan will be tested on at least an annual basis.

9) Physical Security
a) Vendor must employ physical safeguards and visitor access controls to prevent unauthorized access to all systems and media used to process or store ETC sensitive data.
i) Implement video monitoring at all ingress/egress points.
ii) Maintain video for 90 days.

10) Security Policies
a) Vendor must have information security policies that, at a minimum, cover the following topics.
i) Formal assignment of information security is to be given to the Chief Information Security Officer (“CISO”), Information Security Manager, Information Security Group, or another fully dedicated security-knowledgeable member of management.

ii) Creation, distribution, and yearly updating of all information security policies is formally assigned to CISO, Information Security Manager, Information Security Group, or another fully dedicated security-knowledgeable member of management.

iii) Responsibility for monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel is to be formally assigned to the CISO, Information Security Manager, Information Security Group, or another fully dedicated security-knowledgeable member of management.

iv) Responsibility for creating and distributing security incident response and escalation procedures is to be formally assigned to the CISO, Information Security Manager, Information Security Group, or another fully dedicated security-knowledgeable member of management.

v) Responsibility for administering user account, authentication management and access to sensitive data is to be formally assigned to the CISO, Information Security Manager, Information Security Group, or another fully dedicated security-knowledgeable member of management.