Empire State Development Information Technology Policy	No: ESD-IT-CS-007
ESD Vendors, Third-Party Service Providers and Subcontractors Policy	**Original Publication Date: 5/7/2018** **Updated: 5/16/2022** **Issued By:** Issued By: Empire State Development, Information Technology **Owner:** Information Technology **Approver: Carl Harrison**  Vice President Application Development and Chief Information Security Officer **Intended Audience:** Vendors, Third-Party Service Providers and Subcontractors

POLICY SUMMARY

Policies address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities. This policy will establish policy governing security requirements for all ESD Vendors, Third-Party Service Providers and Subcontractors.

INTRODUCTION

ESD Vendors, Third-Party Service Providers and Subcontractors can provide an opportunity for systems to be compromised resulting in the loss of sensitive data and critical business functions. It is important that ESD be able to identify, monitor and mitigate any cyber security risks posed by these relationships.

Vendors, Third-Party Service Providers and Subcontractors must have policies and procedures in place as part of ESD's Security Program. This will mitigate the risk of a cyber security incident as a result of an information security failure by a Vendor and/or Third-Party Service Providers or Subcontractor.

ESD Vendors and Third-Party Service Providers Policy

SCOPE

Vendors, Third-Party Service Providers and Subcontractors may include but are not limited to:

- Law firms
- Accounting firms
- IT service providers
- Federally chartered institutions providing banking services
- Loan servicers
- Licensed persons and companies providing services to insurance companies or brokers
- IT Consultants
- Staffing agencies
- Any other organization that does business with or on behalf of ESD

OBJECTIVES

To "strengthen" the cyber security requirements for Vendors, Third-Party Service Providers and Subcontractors that wish to work with ESD to protect ESD data and client information.

PRINCIPAL

The contractual agreements with Vendors, Third-Party Service Providers and Subcontractors shall state their and the organization's responsibilities for information security

ESD will request cyber security policies from each Vendor, Third-Party Service Provider and Subcontractor.

RESPONSBILITES

Vendors, Third-Party Service Providers and Subcontractors shall where applicable or directed by ESD:

- Sign an NDA or other contractual agreement
- Conduct a background verification checks of all personnel who will have access to data (reference verification is acceptable)
- Notify ESD of any cyber security breaches
- Provide notice to ESD in the event of a cyber security event directly impacting ESD Information Systems or any nonpublic ESD data/information being held by them
- Allow an on-site assessment if requested by ESD
- Provide evidence of
    - due diligence
    - policies and procedures
    - safeguarding sensitive data
    - loss protection
- Incorporate data encryption for personal and sensitive data at rest and in transit
- Implement access controls
- Provide proof and warranties addressing their Cybersecurity policies and procedures that relate to the security of the Information Systems or Nonpublic Information
- Plans and processes must cover at a minimum:
    - Identification of cyber risks
    - Implementation of policies and procedures to protect unauthorized access/use and other malicious acts
    - Detection of cyber security events
    - Responsiveness for cyber security

ESD shall

- All requests for purchases, contracts, services, a new scope of work, or changes to an existing scope of work, that have any form of IT related component or service no matter how small, require the prior involvement and approval of IT. This pertains to all ESD stakeholders, 3rd party vendors and any sub vendors being used.
- Develop relevant guidelines for due diligence and/or contractual protections relating to Vendors, Third-Party Service Providers and Subcontractors including to the extent applicable guidelines addressing information security
- Document all protections against loss incurred as a result of an information security failure by Vendors, Third-Party Service Providers and Subcontractors, including any relevant insurance coverage
- Evaluate (via Vendor/Third Party Provider/Subcontractor confirmation letter and or audit) and monitor the related Vendors, Third-Party Service Providers and Subcontractors controls to ensure that they are acceptably implemented and meet ESD's expectations
- Implement written policies and procedures designed to ensure the security of Information Systems and nonpublic Information that are accessible to, or held by, Vendors, Third-Party Service Providers and Subcontractors
- Determine information security requirements for mitigating the risks associated with their access to ESD's assets. This shall be agreed upon by all parties and documented
- Require Vendors, Third-Party Service Providers and Subcontractors to have policies and procedures for use of encryption to protect nonpublic information in transit and at rest
- Provide Vendors, Third-Party Service Providers and Subcontractors policies and procedures for access controls including use of Multi-Factor Authentication (if applicable) to limit access to sensitive systems and nonpublic information
- Require Vendors, Third-Party Service Providers and Subcontractors to apply information security in accordance with the established policies and procedures of ESD
- Require indemnification clauses in agreements
- Be aware of classification of data that is accessible to them and document the data they are accessing by classification

KEY OUTCOMES

The risks associated with Vendors, Third-Party Service Providers and Subcontractors will be mitigated.

RELATED POLICIES

ESD-IT-CS-001 General Information Technology Policy

POLICY REQUIREMENTS

- Implement written policies and procedures designed to ensure the security of Information Systems and nonpublic information that is accessible to, or held by, Vendors, Third-Party Service Providers and Subcontractors doing business with or on behalf of ESD
- Conduct identification and risk assessment of Vendors, Third-Party Service Providers and Subcontractors
- Determine the minimum cyber security practices required to be met by Vendors, Third-Party Service Providers and Subcontractors in order for them to do business with ESD
- Conduct due diligence processes used to evaluate the adequacy of Cybersecurity practices of such Vendors, Third-Party Service Providers and Subcontractors

- Conduct periodic assessment of such Vendors, Third-Party Service Providers and Subcontractors based on the risk they present and the continued adequacy of their cyber security practices.
- Develop relevant guidelines for due diligence and/or contractual protections relating Vendors, Third-Party Service Providers and Subcontractors in regard to their cyber security practices
- Changes to the provision of services of Vendors, Third-Party Service Providers and Subcontractors, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks
- Conduct identification and risk assessment of Vendors, Third-Party Service Providers and Subcontractors
- Consider insurance policies that would cover information security failures Vendors, Third-Party Service Providers and Subcontractors. The implementation of such a policy is not required by this policy

KEY DEFINITIONS

A Vendor, Third-Party Service Provider or Subcontractor is a person, organization or legal entity other than the principal.

REFERENCES

ISO/IEC 2700:2013 Information Security Management Systems — Requirements

ISO/IEC 27002: 2013 Code of Practice for Information Security Management

ISO/IEC 27003:2017 Information Security Management System Implementation Guidance

NIST SP 800-53 Rev. 4 -1 Security and Privacy Controls for Federal Information Systems and Organizations

ISO/IEC 27005:2011 Information Technology — Security Techniques — Information Security Risk Management

NIST Framework for Improving Critical Infrastructure Cyber Security

NIST Special Publication 800-30, Risk Management Guide

2015 Report released by New York's Department of Financial Services (DFS) detailing the vulnerabilities found in the relationships that many financial institutions had with their third-party vendors

REVISION HISTORY

Revision	Revised By	Date	Description
v1.0 - original	Allyson Burns	5/7/2018	Initial
v2.0	Allyson Burns	5/15/2018	Classification Added
v3.0	Allyson Burns	2/5/2019	Added contractual agreement under responsibilities; Change in title
v4.0	Allyson Burns	6/12/2019	Add additional language
V5.0	Allyson Burns	5/16/2022	Add additional language