ELIZABETH CITY STATE UNIVERSITY
Third-Party/Vendor Risk Management Policy

1. PURPOSE

The purpose of this policy is to ensure that risks associated with Third-Party Service / Vendor Software provider relationships are minimized or eliminated. To ensure Elizabeth City State University (ECSU) applies the appropriate levels of due care and due diligence to validate cybersecurity controls are effective to prevent undue risk ECSU's data and operations.

2. SCOPE

This policy applies to all ECSU faculty and staff, whether full-time or part-time, paid or unpaid, temporary or permanent, volunteers, as well as to all other members of the ECSU community.

3. ACRONYMS / DEFINITIONS

Availability. The measures to which information and critical ECSU services are accessible for use when required.

Confidentiality. The measures to which confidential ECSU information is protected from unauthorized disclosure.

Integrity. The measures to which the accuracy, completeness, and consistency of information is safeguarded to protect the business of ECSU.

Principle of Least Privilege. This principle states a user, program or process should have only the bare minimum privileges necessary to perform its function.

Information Resource. Data, information, and information systems used by ECSU to conduct ECSU operations. This includes not only the information or data itself, but also computer, network, and storage systems used to interact with the information.

Information Asset. Any ECSU-owned and managed equipment used to conduct ECSU operations.

Information System – Any ECSU equipment, applications or systems used to manage, process, or store ECSU's data. This includes, but is not limited to, information systems hosted or managed by third parties.

Information Security. The protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. The focus is on the confidentiality, integrity, and availability of data.

Third-Party Provider / Vendor – Any non-employee of ESCU who is contractually bound to provide some form of product or service to ECSU.

4. POLICY

A. THIRD-PARTY PROVIDER/VENDOR RELATIONSHIPS

i. **Third-Party / Vendor Inventory –** All ECSU departments must develop an inventory of all Third-Party Service Providers, Software Vendors used to store, process or handle ECSU information or data. The inventory must be reviewed and updated annually.

ii. **Third-Party Risk Profile** - All ECSU divisions, with support from the Division of Information Technology, must annually perform a risk-based profile assessment to classify all Third-Party Service Providers into one of three risk categories: High, Medium, or Low. Each risk category must be assigned a specific set of validation requirements which must be jointly defined by the Chief Information Officer, Information Security Officer and Legal Affairs.

iii. **Third-Party Control Assignment** – All ECSU Departments must keep a record of which related controls are to be managed by each Third-Party and which will be handled in-house.

iv. **Third-Party Risk Assessment** – All ECSU departments, in conjunction with the Information Security Officer (or an approved delegate) must conduct an annual review of the information security risks of all third parties with access to ECSU confidential information.

v. **Third-Party Risk Assessment Team** – All ECSU departments must assign responsibility to dedicated staff for performing third-party risk assessments. The team must consist of at least one staff member from ECSU's Division of Information Technology (DIT), Legal Affairs and the Information Security Officer.

vi. **Third-Party Risk Screening** - When using a third-party contractor/consulting services to manage information processing facilities, all risks must be identified in advance, mitigating controls must be established, and all contractor/consulting expectations must be incorporated into the contract agreements for these services.

vii. **Third-Party Information Security Responsibilities** - All ECSU third-party providers must be made aware of their information security responsibilities through specific language appearing in contracts that define their relationship with ECSU.

viii. **Third-Party Security Policy Acknowledge** - All ECSU third-party providers must be made aware of the ECSU Information Security Policies and agree to follow ECSU's policy requirements where applicable.

ix. **Security Requirements in Outsourced Network Services** - All third-party agreements with network service providers must contain defined security requirements so that external networks are at least as secure as ECSU's internal networks.

x. **Third-Party Access Terms and Conditions** - Before any third party is given access to ECSU's systems, a contract defining the terms and conditions of such access must have been signed by the third-party organization and be approved by the respective Vice Chancellor, Information Security Officer and Legal Affairs.

xi. **Third-Party Access Approval** – Granting third-party access to any ECSU internal Information systems that is not clearly public must be approved in advance by the designated Vice Chancellor, Chief Information Officer, and Information Security Officer.

xii. **Right to Approve Personnel for Key Outsourced Positions** – ECSU must have the right to approve or reject any personnel hired by third parties to perform duties on ECSU's premises or handle ECSU's confidential data. This requirement must be included in any contracts with third parties performing information technology or security-related duties for ECSU.

xiii. **Non-Employee Background Checks** – Temporary employees, consultants, contractors, and other third-party organization staff must not be given access to confidential information, or be allowed to access critical information systems, unless they have gone through a background check commensurate with the background checks given to ECSU's employees.

xiv. **Third-Party Notice of Worker Terminations** – If an ECSU terminated employee had authority to direct third-party contractors, or otherwise bind ECSU in a purchase or another transaction, then ECSU management must promptly notify all relevant third parties that the terminated employee is no longer employed by ECSU.

xv. **Personnel Knowledge Transfer with Key Outsourced Positions** - All key technical positions staffed by outsourced personnel must provide cross-training for ECSU in-house personnel for at least six months before contract expiration.

B. SECURITY IN THIRD-PARTY PROVIDER/VENDOR AGREEMENTS

i. **Control Measures in Outsourcing Contracts** - All information technology outsourcing contracts must include specific words defining the control measures that will be provided and maintained. In addition, these contracts must specify a clear and expedient mechanism that ECSU's management can employ to immediately update these controls without bureaucratic delays, protracted negotiations, or outsourcing firm management objections.

ii. **Outsourcing Contract Approvals** - All information-systems-related outsourcing contracts must be reviewed and approved by the appropriate Vice Chancellor, Chief Information Officer, Information Security Officer, Legal Affairs to ensure that these contracts sufficiently define information security responsibilities, how to respond to a variety of potential security problems, and the right to terminate the contract for cause if it can be shown that the outsourcing organization does not abide by the contractual terms.

iii. **Reporting Third-Party Security Violations** - All outsourcing contracts must stipulate that the third parties must notify ECSU's Chief Information Officer and Information Security Officer immediately of any security incident likely to impact confidential ECSU information under their control. ECSU shall retain the right to aid in the investigation of these incidents.

iv. **Outsourcing Security Violations** - All third-party outsourcing contracts must stipulate that the contract may be terminated due to information security violations by the outsourcing third party.

v. **Outsourcing Firm Penalties** - All outsourcing firm contracts must include fiscal penalties, approved by ECSU, for not maintaining information systems controls in a manner consistent with ECSU requirements.

vi. **Service Provider Accountability** - ECSU must ensure service providers acknowledge in writing that they are responsible for the security of confidential data the service provider possesses or otherwise stores, processes, or transmits on behalf of ECSU, or to the extent that they could impact the security of ECSU data.

vii. **Service Provider Acknowledgement -** Service providers must acknowledge in writing to ECSU that they are responsible for the security of confidential data that they possess or otherwise store, process, or transmit on behalf of ECSU, or to the extent that the service provider could impact the security of ECSU.

C. INFORMATION & COMMUNICATIONS TECHNOLOGY SUPPLY CHAIN

i. **Third-Party Confidential Information Handling** - All disclosures of ECSU confidential information to third parties are accompanied by an explicit statement describing exactly what information is restricted and how this information may and may not be used.

ii. **Third-Party Non-Disclosure Agreements** - Prior to sending any confidential information to a third party for copying, printing, formatting, or other handling, the third party must sign an ECSU non-disclosure agreement.

iii. **Receiving Third-Party Information** – If an agent, employee, consultant, or contractor is to receive confidential information from a third party on behalf of ECSU, this disclosure must be preceded by the third party's signing a release form approved by the Legal Affairs.

iv. **Information Handling at Contract Termination** - If ECSU terminates its contract with any third-party organization that is handling ECSU confidential information, this same third-party organization must immediately thereafter destroy or return all ECSU data in its possession.

v. **Third-Party Information Disposal** - If the third party destroys ECSU information, ECSU must receive notice that the data was disposed according to the procedures established or approved by ECSU.

vi. **Supply Chain** - All ECSU departments, with support from the Division of Information Technology, are required to conduct a due care review of third-party providers prior to entering into contractual agreements to acquire information system hardware, software, firmware, or services.

D. MONITORING & REVIEW OF THIRD-PARTY PROVIDER/VENDOR SERVICES

i. **ECSU Divisions,** with support from the Division of Information Technology, establishes a process to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.

ii. **ECSU Divisions** will report weaknesses or deficiencies in supply chain elements as a cybersecurity incident, in accordance with the Incident Response Plan (IRP).

iii. **Independent Security Control Reports** - All agreements with third-party outsourcing organizations stipulates that ECSU will annually receive a report expressing an independent opinion about the adequacy of the controls in use at the outsourcing organization.

iv. **Independent Security Scans of Outsourced Systems** - For all ECSU productions systems managed by third parties, ECSU will hire a qualified, independent third party to validate the security of these systems.

v. **Critical Vendor Financial Review** - The Chief Information Officer (CIO) or designee reviews the financial condition of vendors providing or supporting critical ECSU production information systems annually.

vi. **Third-Party Auditing Agreements** - All agreements dealing with the handling of ECSU information by third parties include a clause granting permission to ECSU for the periodic auditing of the controls used for these information handling activities and specifying the ways in which ECSU information is protected.

vii. **Third-Party Notice of Business and Technical Changes** - Arrangements with information systems outsourcing firms are structured such that respective ECSU divisions and Information Security Officer both receive notices of all material changes in the outsourcing firm business and technical environment. Such notices will be received well in advance of such changes taking effect.

E. MANAGING CHANGES TO THIRD-PARTY SERVICES

i. Changes to the provision of services by third-party providers are managed by ECSU departments, including maintaining and improving existing cybersecurity policies, procedures and controls, taking account of the criticality of business information, systems and processes involved and reassessment of risks and change impact assessment for all changes.

ii. A change control process (involving ECSU Departments and Division of Information Technology) is established and includes, but not limited to, the following:

a. Change Management Roles and Responsibilities between ECSU and the third-party service provider
b. Separation of duties between Change Requesters and Change Implementers
c. Changes are tested and approved prior to Production implementation
d. Impact on the security of data must be assessed for each change

5. PROCEDURES

ECSU shall develop, manage, and review operating procedures to create the proper security posture for protecting ECSU information resources. Such procedures shall be periodically reviewed as required.

6. COMPLIANCE / ENFORCEMENT / SANCTIONS

Any ECSU employee or student found to have violated this policy shall be subject to disciplinary action. Sanctions will be proportionate to the severity and/or frequency of offense and can include termination of employment or expulsion. In addition, violators may be subject to criminal and/or civil action.

7. EXCLUSIONS / EXCEPTIONS

No approved exceptions exist at this time.