Information Technology Department

Third Party Management Policy

Version:	1.2
Effective Date:	08/01/22
Last Reviewed:	5/12/22
Last Approver:	Javornda Ashton
Replaces:	N/A - New

PURPOSE

The purpose of this policy is to mitigate or prevent harm to Northumberland County Public Schools (NCPS) from any service by a vendor, contractor, consultants, software/SaaS providers, managed service providers, or any other individual or Third Party (as defined below.) Third Party management is important to ensure the security of NCPS systems and data.

SCOPE

IT Technicians are responsible for the implantation, review, and management of Third-Party services for NCPS for any non-NCPS personnel or company who:

- Requires any unescorted physical access to secured locations in NCPS properties.
- Requires any unescorted access to NCPS network or systems whether onsite or remote.
- Provides software or applications for NCPS use.
- Provides any hardware or device that connects to the NCPS network which may process, route, or transmit NCPS data.
- Provides any cloud or hosted solution that will host, hold, or process NCPS data.

RESPONSIBILITY

The Director of Educational Technology is responsible for the review, approval, and enforcement of this policy. All personnel who are responsible for the purchase of Third-Party services for NCPS is responsible for adherence to this policy. This policy must be reviewed and updated annually, or when significant changes occur that could impact any safeguard in this policy.

COMPLIANCE

Compliance is expected with all NCPS policies and standards. Policies and standards may be amended at any time. If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a NCPS function, entities shall request an exception through a technology request in the IncidentIQ system at https://ncps.incidentiq.com. Any associate found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

THIRD PARTY MANAGEMENT POLICY

IT is responsible for the classification, inventory, assessment, monitoring, and decommissioning of Third-Party services which may have any impact to IT security or NCPS data. Any person from NCPS wishing to purchase any new system or services from a third-party provider, should work with IT during the IT selection process, and during regularly scheduled third party reviews to ensure proper due diligence is performed to ensure the integrity, confidentiality, and availability of the services.

1. New Third Parties
   - 1.1. IT shall be notified prior to the purchase, acquisition, or use of any new Third Party. Notification to IT should occur through a technology request in the IncidentIQ system at https://ncps.incidentiq.com. .
   - 1.2. Due Diligence
     - 1.2.1. IT shall work with the NCPS personnel requesting the services prior to the purchase of any new Third Party service to review the services to ensure and enforce the security and privacy of NCPS systems and data.
       - 1.2.1.1. IT shall collect information on the Third-Party services and measure the inherent risk to NCPS.
       - 1.2.1.2. IT shall formally review new Third Parties based on their inherent risk to NCPS security and data privacy.
       - 1.2.1.3. IT shall review a current SOC 2 Type 2 report, or similar, for any Third Party that will host any NCPS data.
       - 1.2.1.4. IT shall communicate any risk determined back to the NCPS personnel requesting the services.
     - 1.2.2. IT shall work with the business (if applicable,) and the Third Party, where possible, to ensure contract requirements are included for data security and privacy consistent with NCPS's security program. If the Third Party is part of the major EdTech vendors per the Student Data Privacy Consortium (SDPC), the contract must reference the previous engagements and state that it is expected that the Third Party follows the same rules as NCPS.
2. Existing Third Parties
   - 2.1. IT shall establish and maintain an inventory of all Third Parties used by NCPS. The inventory at minimum shall include, but not be limited to:
     - 2.1.1. Third Party name or identifier
     - 2.1.2. Inherent risk of the Third Party
     - 2.1.3. A specific NCPS contact responsible for the Third Party (business owner)
     - 2.1.4. A summary of the services being provided
     - 2.1.5. A summary of the unmitigated risks of the Third-Party service if applicable.
   - 2.2. IT shall work with the business owner at minimum annually to update the inventory for all Third Parties. This includes ensuring the Third Party is still required, updating the inherent risk of any active Third Party, and ensuring the business owner and use of the vendor has not changed.
   - 2.3. IT shall perform periodic risk assessments on existing Third Parties based on their inherent risk.
   - 2.4. IT shall measure and review Third Party performance based on their inherent risk.

2.5. IT should be involved and review any renewing Third Party contracts for data security and privacy consistent with NCPS's security program. Third Parties which are part of the major EdTech vendors and/or have agreed to the SDPC requirements, should have noted in all contracts that they will abide by the same requirements for NCPS.

2.6. IT should be involved in any contract review where any data security or privacy concerns are raised or discovered for any existing Third Party.

3. Contract Inventory – NCPS should maintain a contract inventory of all Third Parties in use at NDPS.

Definitions of Key Terms

Third Party – Any services by a vendor, contractor, consultants, software/SaaS providers, managed service providers, or any other individual who:

- Requires any unescorted physical access to secured locations in NCPS properties.
- Requires any unescorted access to NCPS network or systems whether onsite or remote.
- Provides software or applications for NCPS use.
- Provides any hardware or device that connects to the NCPS network which may process, route, or transmit NCPS data.
- Provides any cloud or hosted solution that will host, hold, or process NCPS data.

Policy References to IT Standards

K-12 Model Security Plan V1.0 – For the second calendar year running, at least 75 percent of all data breach incidents affecting U.S. public K-12 school districts were the result of security incidents involving school district vendors and other partners.

K-12 Model Security Plan V1.0 – Software Approval Processes - Establish a vetting and approval process for an approved software inventory.

K-12 Model Security Plan V1.0 – Inventory - A complete inventory of devices, assigned users, contract and purchase information should be available.