POLICY

Purpose

To establish a framework for managing software and technology vendors that ensures the security, reliability, and compliance of Ocean County College's (OCC) digital infrastructure.

Scope

This policy applies to all software and technology vendors that provide products or services which interact with OCC systems, networks, or data. It covers both OCC-managed systems and any external platforms that interconnect with or exchange data with OCC infrastructure.

Policy Statement

Ocean County College engages with external software and technology vendors to support institutional operations. These engagements must be governed by standards that protect OCC's data and systems from unauthorized access, modification, and destruction.
To maintain a secure and resilient environment, OCC will:

- Require vendors to meet minimum cybersecurity standards
- Evaluate vendors prior to engagement through a defined approval process
- Align vendor oversight with applicable laws and frameworks, including:
    - Gramm-Leach-Bliley Act (GLBA)
    - NIST SP 800-171, Revision 3
    - NIST Cybersecurity Framework (CSF)
    - New Jersey Administrative Code Title 15, Chapter 3 – Records Retention

The IT Governance Council, in collaboration with Procurement Services and relevant departments, is responsible for oversight and enforcement of this policy.

Exceptions

Exceptions must be documented and approved by the IT Governance Council. Each exception must include a justification and a risk mitigation plan. Exceptions may apply to legacy systems, third-party platforms not under OCC's direct control, or systems lacking full oversight capabilities.

ADOPTED: October 9, 2025

PROCEDURE

Objective

To define operational procedures for evaluating, onboarding, and managing software and technology vendors in accordance with OCC's policy.

1. **Vendor Evaluation**
   - Vendors must submit documentation of their internal security posture, including written policies and results from independent assessments (e.g., third-party audit reports or certifications).
   - Vendors must be reviewed and approved by IT Governance, Procurement Services, and the requesting department before engagement.
2. **Security Awareness and Access**
   - Vendor personnel accessing OCC systems must complete basic security awareness training as defined by OCC IT.
   - Access will be granted through standard user accounts only, following acceptance of OCC's Acceptable Use Policy.
3. **Approved Access Methods**
   - Vendors must use OCC-approved methods for remote access, such as secure network connections and multi-factor authentication.
   - Use of external remote access tools or software must undergo a security assessment and receive prior approval from OCC IT.
4. **Access Restrictions and Auditing**
   - Vendors will not be granted privileged accounts.
   - Access permissions will be limited to contractual requirements.
   - All vendor account activity will be logged and audited per OCC's Audit and Accountability Policy.
5. **Revocation of Access**
   - OCC IT may revoke or modify vendor access at any time if inappropriate activity is suspected or if the vendor poses a security risk.
6. **Incident Reporting**
   - Vendors must report any security incidents that may impact OCC, including breaches, cyberattacks, legal investigations, or infrastructure failures.
   - Incidents must be reported immediately, but no later than three (3) business days after discovery.
   - Any event that significantly impacts the functionality or availability of the vendor's product or service used by OCC must also be reported.
   - Reports must include relevant details such as nature of the incident, affected systems, and remediation steps.

ADOPTED: October 9, 2025