Service Level Agreement (SLA) for Security Services

Related Policies, Procedures, or Standards:
VSCS Acceptable Use Policy
VSCS Firewall Policy
VSCS Incident Response Policy
VSCS Password and Access Management Policy
VSCS Security Awareness Policy
Keywords/Categories:
Security, cyber security, incident response, vulnerability, firewall, backup, recovery

1 General Overview

This is an SLA between IT Shared Services and the member institutions of the Vermont State Colleges (VSC) system. This agreement outlines the information security services offered and is intended to document procedures for security services and set service level expectations for these services. Service level commitments are specified. The agreement is effective as of the Effective Date set forth and will continue until revised or terminated.

For the purposes of this SLA, "customer" is defined collectively as the Community College of Vermont, Vermont State University, Workforce Development, and the Chancellor's Office, plus any other Vermont State Colleges (VSC) entity whose inclusion may be negotiated. The "end-user" is defined as VSC faculty, staff, student, guest, or any other user of this service.

2 Service Description

2.1 Service Scope

The scope of this service is for the provision of information security, network security, and cybersecurity services.

Services include:

- Vendor (3rd Party) Security Reviews
- Access control policy
- Contract and HECVAT review
- Critical system recovery plans
- Education and testing
- Incident response
- Security operations
- Virus and malware protection
- Vulnerability management
- Working with cyber insurance provider

- Tracking security trends/best practices

2.2 End-User Requirements to Use the Service

- End-users will be expected to comply with relevant guidelines, policies, and procedures to help ensure enterprise-wide security;
- Compliance with IT policies including (but not limited to) those listed at the beginning of this SLA;
- In the case of an incident investigation, users will follow direction from staff to facilitate discovery.

2.3 Boundaries of Service Features and Functions

- IT Shared Services will evaluate compliance with the following regulatory, contractual, or policy requirements:
    - Family Education Rights and Privacy Act (FERPA);
    - Health Insurance Portability and Accountability Act (HIPAA);
    - Gramm Leach Bliley Act aka Financial Services Modernization Act (GLBA);
    - Payment Card Industry (PCI).
- Security tools and assessments are based on known threats. There are many unknown threats, such as variations in ransomware and zero-day exploits that are designed not to be detected and may get past our tools.

3 Service Level Performance

- Security incidents are prioritized based on their impact to the organization;
- There are no specific service levels beyond that of the IT Shared Services SLA. Due dates can be set by agreement on individual requests;
- Self-service password reset is available 24 hours a day, except during maintenance events.

3.1 IT Shared Services Responsibilities in Support of the Service

- Meet response times associated with the priority assigned to incidents and service requests;
- Comply with state and federal laws, as well as with VSC policies, to escalate to appropriate authority once a crime, breach, or security incident is reported or evidence of same is present;
- Communicate any changes to priority that occur due to incident response;
- Provide friendly, courteous, and efficient service;
- Provide end-user education on security awareness and best-practices;
- Promptly refer any inquiries/complaints to the appropriate responsible team.

3.2 Customer Responsibilities in Support of the Service

- IT governance groups to collaborate with IT Shared Services IT on the service framework to satisfy the Vermont State Colleges business requirements;
- Comply with the SLA and follow process for escalation if services are not being met.

4 Hours of Coverage and Escalation

4.1 Hours of Coverage

Security services hours of coverage are 24x7x365. Outside of regular Monday-Friday, 8:00 AM to 5:00 PM, services are limited and emergency only.

4.2 Service Exceptions to Coverage

No exceptions listed.

4.3 Escalation and Exceptions

If you are not satisfied with the performance of the service or incident/request process, please contact the Service Owner or Service Manager.

IT Shared Services Contacts

Service Owner	Name: Tony Hashem Title: Information Security Officer Phone: 802-498-7936 Email: Tony.Hashem@vsc.edu
Service Manager	Name: Ken Bernard Title: Information Security Operations Lead Phone: 802-698-3048 Email: ken.bernard@vsc.edu

To request exceptions to defined service levels based on exceptional business needs, please email cio@vsc.edu. The Office of the CIO/IT Shared Services will respond to the message within 5 business days and escalate any mutually agreed upon exceptions for review, approval, and funding, if necessary.

5 Service Requests

A Service Request is defined as a request for information, advice, or for access to a service.

5.1 Service Request Submission

Service Requests can be submitted by creating a support ticket in ServiceDesk.

5.2 Service Request Response

For all requests, IT Shared Services' objective is to acknowledge and assign requests within 12-24 business hours of receipt. Requests will be fulfilled within seven (7) days. Campus priorities may require exceptions during certain times of the Academic year.

6 Incidents

An incident is defined as any interruption in the normal functioning of a service or system.

6.1 Incident Report

Phishing emails can be reported by forwarding the email to cybersecurity@vsc.edu. All other incidents can be reported by contacting the support desk or creating a support ticket in ServiceDesk.

6.2 Incident Response

Refer to Incident Response Policy

6.3 Prioritization

All reported incidents receive a priority number based on the impact and urgency of the service interruption. Impact is determined based on the number of people/departments/buildings that are affected by the interruption or outage. Life-Safety issues are taken into consideration for assessing and assigning priorities. Urgency is based on the acceptable delay to restore the service. Urgency can be critical or high and is determined based on the nature of the service outage.

IT Shared Services may prioritize incoming security incident requests as priority if it meets one or more of the following criteria:

- Significant number of people affected;
- The level to which work is impaired for individuals;
- Loss or theft of sensitive information (Ex. PII, PHI, Financial);
- Cyber-attacks on organization infrastructure or websites;
- Cyber Extortion.

7 Maintenance and Service Changes

The Maintenance Window for Security can be found on the IT Shared Services website.

IT Shared Services reserves the right to modify the maintenance window.

8 Performance and Review

8.1 System Performance and Availability

Service performance and availability reports will be provided with the release of the annual report.

8.2 SLA Reviews

Shared Services IT is responsible for facilitating reviews of this document. Contents of this document may be amended as required, provided mutual agreement is obtained from the primary stakeholders and communicated to all affected parties. This SLA contains the complete

agreement between the parties and shall not be changed, amended, or altered except in writing and signed by each party.

Signatures

Revision History

Date	Revision	Revised By	Signature
12/21/2022	Original Draft	Meg Walz	
1/16/2025	Revised	Gayle Malinowski