SUNSET RIDGE SCHOOL DISTRICT 29
525 SUNSET RIDGE RD
NORTHFIELD, IL 60093

Education Committee Meeting:

Tuesday, September 15, 2020 – 6:00 p.m. at Sunset Ridge School (525 Sunset Ridge Road. Northfield, IL. 60093)

SUNSET RIDGE SCHOOL DISTRICT 29
525 Sunset Ridge Road • Northfield, Illinois • 60093
847 881 9400 • Fax: 847 446 6388 • www.sunsetridge29.org
Cultivating a learning community that engages the hearts and minds of students, one child at a time

BOARD OF EDUCATION
SUNSET RIDGE SCHOOL DISTRICT 29
525 SUNSET RIDGE ROAD
NORTHFIELD, ILLINOIS 60093
EDUCATION COMMITTEE MEETING
SEPTEMBER 15, 2020
6:00 p.m.

Join Zoom Meeting https://us02web.zoom.us/j/89323871079 .Meeting ID: 893 2387 1079

Public comments should be submitted in writing to stangee@sunseridge29.org no later than 9 a.m.. on September 15, 2020.

AGENDA

1. ROLL CALL

2. APPROVAL OF MINUTES
   2.1 Minutes from May 12, 2020 Meeting

3. PUBLIC COMMENT

4. REPORTS
   4.1 Discussion: Technology Audit Update

5. NEXT MEETING: November 10, 2020

6. ADJOURNMENT:

D29 NETWORK & SYSTEMS SECURITY UPDATE SEPTEMBER 2020

Director of Technology & Innovation — Sheri Styczen
Network & Data Security Manager — Brian Thiel

NETWORK & SYSTEMS SECURITY UPDATE
(CURRENT PRACTICE AND OPTIONS FOR ENHANCEMENTS)

- Student Online Personal Protection Act (SOPPA) Update
- Staff Information Security Awareness Training
- Physical Access to Network Rooms
- Device Management & Security
- Network Security
- Policy/Procedures Recommendations

Student Online Personal Protection Act (SOPPA) Update

STUDENT ONLINE PERSONAL PROTECTION ACT - SOPPA

Current Practice

- Review all contracts and privacy policies before implementing a new subscription

Options for Enhancements

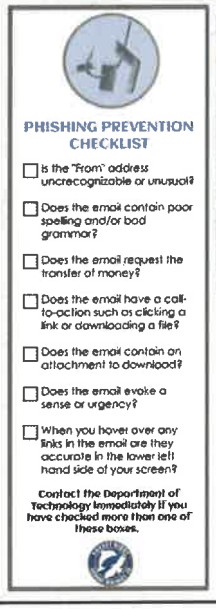
- Recent amendments to the Illinois Student Online Personal Protection Act (SOPPA) go into effect on July 1, 2021.
- List of requirements for Districts to post online.

Staff Information Security Awareness Training

INFORMATION SECURITY AWARENESS TRAINING

Current Practice

- Implemented KnowBe4 in 2017
- Paper bookmark
- HALO Phishing test - recommended by CLIC
- Quarterly Phishing Training Campaigns



PHISHING PREVENTION CHECKLIST

- ☐ Is the "From" address unrecognizable or unusual?
- ☐ Does the email contain poor spelling and/or bad grammar?
- ☐ Does the email request the transfer of money?
- ☐ Does the email have a call-to-action such as clicking a link or downloading a file?
- ☐ Does the email contain an attachment to download?
- ☐ Does the email evoke a sense or urgency?
- ☐ When you hover over any links in the email are they accurate in the lower left hand side of your screen?

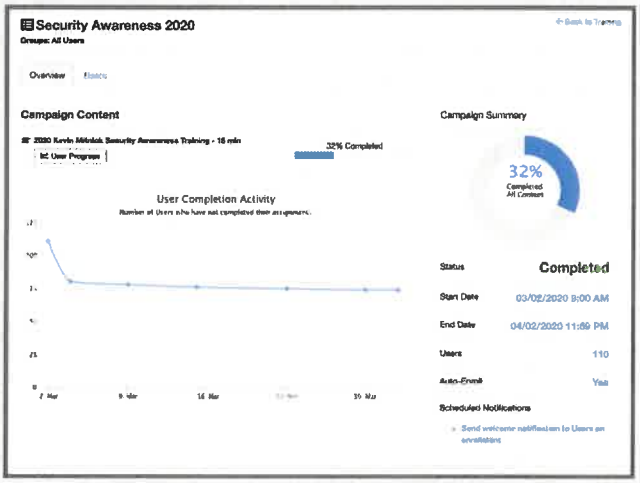
Contact the Department of Technology immediately if you have checked more than one of these boxes.

Education	444	3/10/19
Threat Cluster	Incidents	Percent of Incidents
Personnel Error	241	54%
Hacking System	231	52%
Social Engineering	117	26%
Personnel Misuse	113	25%
Physical Asset Loss	103	23%
Hacking Web	102	23%
Malware	76	17%
Physical Facility	56	13%
System Failure	2	0%
POS	1	0%

INFORMATION SECURITY AWARENESS TRAINING CONT.

Option For Enhancements

- Mandated Information Security Awareness Training for ALL Staff to prevent and respond to potential intrusions.
  - Sample



****Recommended as a result of the Network Risk Assessment**

Physical Access to the Network

PHYSICAL ACCESS

Current Practice

- Physical key access to all server rooms
- No access monitoring system in place

Option For Enhancements

- **Key Fob all network rooms/closets for access monitoring

****Recommended as a result of the Network Risk Assessment**

Device Management and Security

DEVICE MANAGEMENT

Current Practice

MacBook Pro Management
- Tech Dept pushes out updates
- Tech Dept pushes out apps

Chromebook Management
- Google Admin Console

Business Office
- Windows Devices that are not managed

Options for Enhancements
- Purchase MacBooks for the Business Office
- Purchase a Windows server and software (in addition to training)
- Do nothing

Network Security

SECURITY INFORMATION & EVENT MANAGEMENT

Current Practice

- Intrusion Detection
- Intruder Prevention
- Malware Detection
- Antivirus
- Built in Security through managed platform (all but Business Office machines)

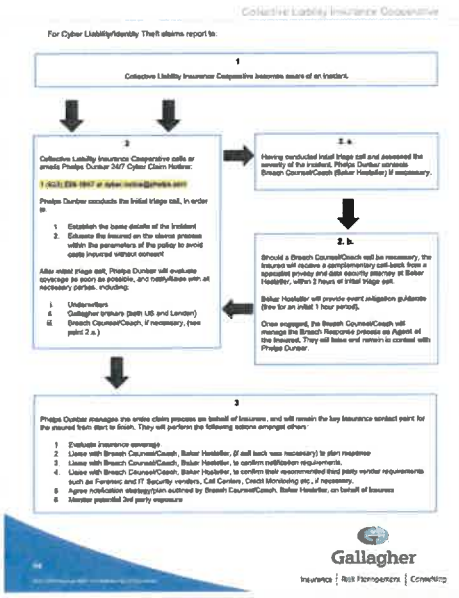
Options for Enhancements

- Product that takes all log files from every device and looks anomaly and makes a determination if our system is being compromised
- 3rd Party company to monitor traffic entering and leaving the District

SEEKING OUTSIDE INVESTIGATION

Current Practice

- When we become uncomfortable with the malware that is installed, we recommend passing it on for a 3rd party opinion
- If PII was accessible on the device



OPTIONS FOR ACTIVE MONITORING

Intrusion Detection

- Purchase monitoring from an outside company

Device Management

- Move all Business Office users to MAC to manage their devices

---

Prevent Need for Active Monitoring Through Improved Data Management for Sensitive Data

- Leave it in District
- Send sensitive Business Office files to an off-site active storage with synchronous usage

POTENTIAL IMPROVEMENTS & COSTS

SOPPA Notices on Website	$0
Staff Training (Protocols to prevent and respond)	$0
Install Fobs for Network Closet Monitoring	$15,000
BO to Apple Devices (MacBook Pros)	$6000
Security Monitoring	$100,000
Annual Renewal	$80,000
Outsourced Investigation (per incident)	$15,000
Offsite Storage for Business Office Sensitive Files	$10,000

QUESTIONS

LEGISLATION BRIEF

Student Online Personal Protection Act (SOPPA) Changes

EXECUTIVE SUMMARY

Effective July 1, 2021, school districts will be required by the Student Online Personal Protection Act (SOPPA) to provide additional guarantees that student data is protected when collected by educational technology companies, and that data is used for beneficial purposes only (105 ILCS 85).

Note that SOPPA also places new expectations on the Illinois State Board of Education and operators of online services or applications.

DISTRICT REQUIREMENTS

Below is a high-level overview of the new requirements. Please refer to the legislation for specific timelines and components of each element.

School districts must:

1. Annually post a list of all operators of online services or applications utilized by the district.
2. Annually post all data elements that the school collects, maintains, or discloses to any entity. This information must also explain how the school uses the data, and to whom and why it discloses the data.
3. Post contracts for each operator within 10 days of signing.
4. Annually post subcontractors for each operator.
5. Post the process for how parents can exercise their rights to inspect, review and correct information maintained by the school, operator, or ISBE.
6. Post data breaches within 10 days and notify parents within 30 days.
7. Create a policy for who can sign contracts with operators.
8. Designate a privacy officer to ensure compliance.
9. Maintain reasonable security procedures and practices. Agreements with vendors in which information is shared must include a provision that the vendor maintains reasonable security procedures and practices.

Although not required by law, school districts will also need to undertake the following to meet the above requirements:

- Provide teachers with the list of online operators that are safe and approved for use.
- Develop a process for keeping data inventory up-to-date.

Information Security Awareness Training Policy

Purpose and Summary

This document establishes the Information Security Awareness Training Policy for the University of Arizona. This policy ensures security awareness and training controls that protect the confidentiality, integrity, and availability of the University's Information Resources.

Scope

This policy applies to all Information Systems and Information Resources owned or operated by or on behalf of the University. All University-Related Persons with access to University Information or computers and systems operated or maintained on behalf of the University are responsible for adhering to this policy.

Definitions

CISO: The senior-level University employee with the title of Chief Information Security Officer.

Elevated Access: A level of access that is authorized to perform functions that ordinary users are not authorized to perform.

Information Owner: The individual(s) or Unit with operational authority for specified University Information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. This individual or Unit is responsible for making risk tolerance decisions related to such Information on behalf of the University and is organizationally responsible for any loss associated with a realized information security risk scenario.

Information Resources: University Information and related resources, such as equipment, devices, software, and other information technology.

Information System: A major application or general support system for storing, processing, or transmitting University Information. An Information System may contain multiple subsystems. Subsystems typically fall under the same management authority as the parent Information System. Additionally, an Information System and its constituent subsystems generally have the same function or mission objective, essentially the same operating characteristics, the same security needs, and reside in the same general operating environment.

Information System Owner: The individual(s) or Unit responsible for the overall procurement, development, integration, modification, and operation and maintenance of an Information System. This individual or Unit is responsible for making risk tolerance decisions related to such Information Systems on behalf of the University and is organizationally responsible for the loss, limited by the bounds of the Information System, associated with a realized information security risk scenario.

ISO: The University's Information Security Office, responsible for coordinating the development and dissemination of information security policies, standards, and guidelines for the University.

Unit: A college, department, school, program, research center, business service center, or other operating Unit of the University.

University Information: Any communication or representation of knowledge, such as facts, data, or opinions, recorded in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual, owned or controlled by or on behalf of the University.

University-Related Persons: University students and applicants for admission, University employees and applicants for employment, Designated Campus Colleagues (DCCs), alumni, retirees, temporary employees of agencies who are assigned to work for the University, and third-party contractors engaged by the University and their agents and employees.

User: Individual or group that interacts with a system or benefits from a system during its utilization.

Policy

A. All Classifications of University Information

1. ISO, on behalf of the University, must define and ensure the implementation of an information security awareness training program to increase Users' awareness of their information security responsibilities in protecting the confidentiality, integrity, and availability of University Information Resources.

2. Employee and DCC Security Awareness Training
    a. All University employees (including student employees) and Designated Campus Colleagues (DCCs) with access to University Information Resources must complete security awareness training within the first 30 days from date of hire. Information Security

Refresher Training must be completed annually, within 60 days of the anniversary of the previous instance of such training.

3. Role-Based Security Awareness Training
   a. Additional role-based security awareness training must be required for employees and DCCs whose responsibilities require Elevated Access, including access to Regulated or Confidential Information, as defined in the University's Data and Classification Handling Standard [2] (e.g., information subject to additional requirements under HIPAA, PCIDSS, FISMA, ITAR/Export Control, NIST 800-171), and related Information Systems. Role-based training must be completed on an annual or periodic basis, as required by the relevant regulatory or contractual compliance programs.

Compliance and Responsibilities

Compliance

Tracking, Measuring, and Reporting

ISO must initiate mechanisms for tracking compliance with this policy and must produce reports representing these measures to support University decision making. Recourse for Noncompliance ISO is authorized to limit network access for individuals or Units not in compliance with all information security policies and related procedures. In cases where University resources are actively threatened, the CISO should act in the best interest of the University by securing the resources in a manner consistent with the Information Security Incident Response Plan. In an urgent situation requiring immediate action, the CISO is authorized to disconnect affected individuals or Units from the network. In cases of noncompliance with this policy, the University may apply appropriate employee sanctions or administrative actions, in accordance with relevant administrative, academic, and employment policies.

Exceptions

Requests for exceptions to any information security policies may be granted for Information Systems with compensating controls in place to mitigate risk. Any requests must be submitted to the CISO for review and approval pursuant to the exception procedures published by the CISO.

Frequency of Policy Review

The CISO must review information security policies and procedures annually, at minimum. This policy is subject to revision based upon findings of these reviews.

Responsibilities

University-Related Persons

All University-Related Persons are responsible for complying with this policy and, where appropriate, supporting and participating in processes related to compliance with this policy.

Information Owners and Information System Owners

Information Owners and Information System Owners are also responsible for implementing processes and procedures designed to provide assurance of compliance with the minimum standards, as defined by ISO, and for enabling and participating in validation efforts, as appropriate.

Regulatory and Contractual Compliance Programs

Regulatory and Contractual Compliance Programs that are responsible for ensuring appropriate treatment of Regulated or Confidential Information must establish additional role-based security awareness training modules specific to their program, along with accompanying periodicity requirements.

Chief Information Security Officer

ISO must, at the direction of the CISO:

- identify solutions that enable consistency in compliance and aggregate and report on available compliance metrics;
- develop, establish, maintain, and enforce information security policy and relevant standards and processes;
- provide oversight of information security governance processes;
- educate the University community about individual and organizational information security responsibilities;
- measure and report on the effectiveness of University information security efforts; and
- delegate individual responsibilities and authorities specified in this policy or associated standards and procedures, as necessary.

Vice Presidents, Deans, Directors, Department Heads, and Heads of Centers

All Vice Presidents, Deans, Directors, Department Heads, and Heads of Centers must take appropriate actions to comply with information technology and security policies. These individuals have ultimate responsibility for University

resources, for the support and implementation of this policy within their respective Units, and, when requested, for reporting on policy compliance to ISO. While specific responsibilities and authorities noted herein may be delegated, this overall responsibility may not be delegated.

Related Information*

ISO Website [3]
Information Security Policy (IS-100) [4]
Data Classification and Handling Standard [5]
Designated Campus Colleague Quick Reference Matrix [6]

Revision History*

Nonsubstantive revisions January 24, 2020

Replaces Interim policy of 3/19/19

Source URL:
https://policy.arizona.edu/information-technology/information-security-awareness-training-policy

Links

[1] mailto:security@arizona.edu
[2] https://security.arizona.edu/content/data-classification-and-handling-standard
[3] https://security.arizona.edu/content/policy-and-guidance
[4] http://policy.arizona.edu/information-technology/information-security-policy
[5] https://security.arizona.edu/data-classification-and-handling-standard
[6] https://hr.arizona.edu/sites/default/files/hr/Workforce-Systems/uaccess-resources/dcc/DCC_Srvc_Mat rix.pdf