Haida Gwaii School District

Information Technology Working Model

School District No. 50
Haida Gwaii

Security Framework

Within School District No. 50 (Haida Gwaii), our efforts are directed towards establishing a zero-trust environment. Zero Trust is a security framework requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data. Zero Trust assumes that there is no traditional network edge; networks can be local, in the cloud, or a hybrid model with resources anywhere, as well as having users in any location. Zero Trust is a framework for securing infrastructure and data for today's modern digital transformation. It uniquely addresses the modern challenges of today's business, including securing remote workers, hybrid cloud environments, and ransomware threats.

- **Data Security**: Educational institutions handle sensitive information about students, teachers, and staff. Adopting a zero-trust model ensures that data isprotected from unauthorized access or breaches, reducing the risk of data leaks.
- **Increasing Cyber Threats**: With the rise in cyber threats and attacks on organizations, including schools and educational systems, implementing a zero-trust environment helps mitigate the risk of unauthorized access, data breaches, and other cybercrimes.
- **Protecting Personal Identifiable Information (PII)**: Educational records often contain personally identifiable information (PII) of students and staff. A zero-trust approach ensures that access to this sensitive information is strictly controlled and monitored to prevent unauthorized use or disclosure.
- **Device Proliferation:** With the increasing use of various devices in educational settings, such as laptops, tablets, and smartphones, a zero-trust approach helps in securing access from different devices, regardless of their location.
- **User Accountability**: Zero trust requires continuous verification of users and devices. This approach enhances user accountability and ensures that individuals accessing the network are authenticated and authorized, reducing the risk of insider threats.
- **Device-Centric Security**: In a one-to-one device environment, where each user has their own device, a zero-trust model focuses on securing the device itself. It ensures that only authorized and properly configured devices can access the network, reducing the risk of compromised or unauthorized devices.
- **Continuous Authentication**: Zero trust involves continuous authentication, meaning that user identities are verified throughout their entire session. This constant validation is crucial in one-to-one device scenarios, where users might move between locations or share devices, ensuring that access remains secure regardless of the device's physical location.
- **Adaptive Access Control**: Zero trust employs adaptive access controls, adjusting permissions based on real-time assessments of user behavior and device health. This flexibility is essential in a one-to-one device setting, accommodating various usage patterns and adapting security measures accordingly.
- **Protecting Sensitive Data**: In educational settings with one-to-one devices, there's often a significant amount of sensitive student and faculty data. Zero trust ensures that access to this data is tightly controlled, reducing the risk of data breaches and unauthorized access, fostering a secure learning environment.
- **Securing Remote Access**: As one-to-one devices are frequently used for remote learning, a zero-trust model provides a robust framework for securing remote access. It verifies the user and device regardless of their location, crucial for maintaining security in an environment where remote access is prevalent.
- **Compliance Requirements:** Educational institutions often need to comply with data protection and privacy regulations. A zero-trust model helps meet these compliance requirements by providing a comprehensive and proactive security approach.
-

In summary, a zero-trust environment for School District 50 Haida Gwaii, is essential to protect sensitive data, comply with regulations, and address the evolving cybersecurity landscape, especially in the context of increased digitalization.

One-to-one

Previous IT model

Year 1	Gudangaay Tlaats'gaa Naay	$35,000	Agnes L. Mathers	$15,000
Year 2	Sk'aadgaa Naay	$30,000	Tahayghen Elementary	$20,000
Year 3	GidGalang Kuuyas Naay	$35,000	Port Clements Elementary	$15,000

In the updated one-to-one model, the annual contribution from the six schools, totalling **$50,000**, is combined with an additional **$40,000** from the school district, resulting in a comprehensive budget of **$90,000** per year. This budget is structured to support a full cycle refresh every six years. At the conclusion of the six-year period, the total accumulated refresh budget would reach **$540,000**. These funds are earmarked for the acquisition of new devices, benefiting both teachers and students. Approximation below.

Teachers	Students
50 Devices $85,841.70	450 Devices $454,652.10
	Total $540,493.80

Guiding Principles - Refresh

When it comes time to refresh the one-to-one staff and student devices, this will be guided by the following criteria.

- Ministry Requirements
- Current Technology Infrastructure
- Accessibility for Users
- Security
- Budget

Schools' responsibilities
The school will be responsible for the costs associated with any lost or damaged devices, as the one-to-one program does not generate revenue. Additionally, the school will need to provide funds for office staff computers, printing devices, school TVs, Apple TVs, and specialized software, if required.

Cell Phones
The schools are responsible for the costs associated with cell phones. In the event that there are overage charges such as data, overuse and roaming passes, these charges will be billed directly to the user. To receive special rates when purchasing a cell phone, the purchase must be through the school district office.

Current Monthly Plan
Unlimited (Canada)
Unlimited Texting (Canada)
5GB Data

App Request

1. Reach out to SD50 IT staff by email or phone to discuss app.

2. Gather the following general information:
   - Name
   - Privacy Statement (usually found on the App website)
   - Internet Connectivity needed – Yes or No
   - Is it compatible with 7th generation IPADs
   - Cost - Is this a Site License based app? How will costs be covered? Is there an existing budget code?

3. Educational Purpose:
   - In your request, emphasize how the app contributes to student learning. Be specific regarding relevance to curriculum, learning goals, engagement, subject area, productivity, creativity, etc.
   - Explain how the existing apps on the devices fail to align with your objectives.

4. Send the above to SD50 IT Department

All new apps must undergo a privacy scan before receiving approval. During this scan, any findings may trigger the need for a Privacy Impact Assessment (PIA).

Section 69 (5) of the Freedom of Information and Protection of Privacy Act (FOIPPA) requires you to conduct a PIA. You need a PIA to determine whether your project involves personal information and if so, how you'll protect the information you collect or use in your project.

Requesting an app does not guarantee approval for use in your school. Several factors, including privacy, security, cost, and existing alternatives, are considered when adding new apps. Location based apps, and Apps with built-in advertising will not be considered.

**Please be aware that adding an app means that it is added to all IPADS in the group, which typically means the school.*

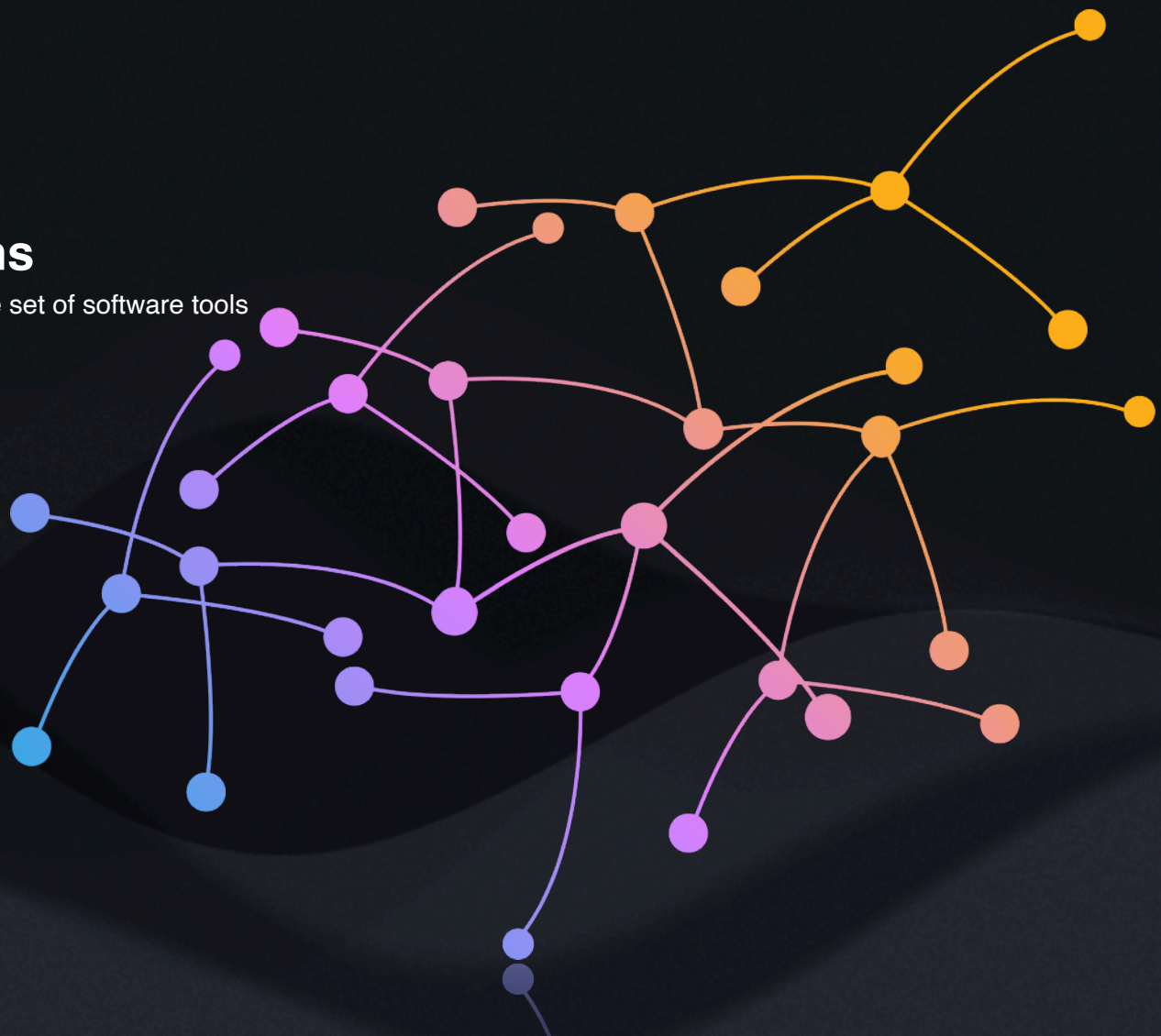
District’s responsibility

The district oversees the maintenance and cost of network connectivity, including switches, routing, security cameras, landline communication hardware, NVRs, device charging stations and Wi-Fi systems to ensure optimal performance and reliability across the educational environment. This commitment fosters a technologically robust infrastructure, facilitating efficient communication and supporting learning. Regular monitoring, updates, and troubleshooting are essential to adapt the network to evolving educational needs, emphasizing the district's dedication to a reliable and advanced educational ecosystem. Additionally, the district manages licensing costs and the Mobile Device Management platform, further demonstrating its comprehensive responsibility for the technological aspects of education.

District’s provided platforms

The district is committed to provide a comprehensive set of software tools to teachers and students. The tools provided are.

Microsoft 365 A3 license
Apple School Manager
Google Workspace
Cisco Umbrella DNS Protection



Incident Response

Purpose
The purpose of this plan is to define the roles, responsibilities, procedures, and tools for responding to and managing security incidents that affect our organization's information systems and assets.

Scope
This plan applies to all employees, contractors, and third-party vendors who have access to our organization's network, systems, devices, and data. It covers all types of security incidents, such as data breaches, denial-of-service attacks, malware infections, unauthorized access, theft, vandalism, and natural disasters.

Objectives
The objectives of this plan are to:

- Protect the confidentiality, integrity, and availability of our information and systems
- Minimize the impact and damage of security incidents
- Restore normal operations as quickly as possible
- Identify the root causes and lessons learned from security incidents
- Improve our security posture and resilience

Roles and Responsibilities
The following roles and responsibilities are assigned to the members of the incident response team:

Incident Manager: The incident manager is the leader of the incident response team and the main point of contact for all incident-related communications. The incident manager is responsible for coordinating the incident response activities, assigning tasks, making decisions, escalating issues, and reporting to senior management and stakeholders.
The incident manager would be determined on the type of incident.

Technical Lead: The technical lead is the expert on the technical aspects of the incident response.
The technical lead is responsible for analyzing the incident, containing the threat, eradicating the source, restoring the systems, and preserving the evidence. this could be a third-party brought in to utilize their expertise.

Communications Lead: The communications lead is the spokesperson for the incident response team and the liaison with the internal and external parties. The communications lead is responsible for developing and delivering the incident response messages, updating the status, and managing the expectations of the employees, customers, partners, media, and regulators.

Legal Counsel: The legal counsel is the advisor on the legal and regulatory implications of the incident response.
The legal counsel is responsible for reviewing and approving the incident response communications, ensuring the compliance with the applicable laws and standards, and handling any legal disputes or claims arising from the incident.
Other Support Staff: The other support staff are the additional resources that the incident response team may need to assist with the incident response. The other support staff may include IT staff, security staff, human resources staff, finance staff, and external consultants or vendors.

Incident Response Process
The incident response process consists of six phases: preparation, identification, containment, eradication, recovery, and lessons learned.

Preparation
The preparation phase involves the activities that the incident response team performs before an incident occurs to ensure readiness and effectiveness. These activities include:

- Developing and updating the incident response plan procedures.
- Establishing and training the incident response team.
- Acquiring and maintaining the incident response tools and equipment
- Conducting regular backups and testing of the critical systems and data
- Performing risk assessments and vulnerability scans of the network and systems
- Implementing security controls and best practices to prevent or mitigate incidents

Identification
The identification phase involves the activities that the incident response team performs to detect and confirm an incident. These activities include:

- Monitoring and analyzing the network and system logs, alerts, and events
- Investigating and verifying the signs and symptoms of an incident
- Determining the scope, severity, and impact of an incident
- Classifying and prioritizing the incident according to the predefined criteria
- Reporting and escalating the incident to the appropriate parties

Containment
The containment phase involves the activities that the incident response team performs to isolate and stop the spread of an incident. These activities include:

- Disconnecting or blocking the affected network segments, systems, or devices
- Applying patches or updates to the vulnerable or compromised systems
- Changing the passwords or credentials of the affected accounts or users
- Implementing firewall rules or access control lists to restrict the network traffic
- Collecting and securing the evidence for further analysis

Eradication
The eradication phase involves the activities that the incident response team performs to eliminate the root cause and source of an incident. These activities include:

- Identifying and removing the malicious files, code, or data
- Cleaning or restoring the infected or corrupted systems or devices
- Scanning and verifying the network and systems for any remaining traces of the threat
- Documenting and reporting the findings and actions of the eradication phase

Recovery
The recovery phase involves the activities that the incident response team performs to restore the normal operations and functionality of the network and systems. These activities include:

- Reconnecting or unblocking the isolated network segments, systems, or devices
- Testing and validating the functionality and performance of the restored systems
- Monitoring and verifying the security and stability of the network and systems
- Communicating and updating the status and resolution of the incident to the relevant parties

Lessons Learned

The lessons learned phase involves the activities that the incident response team performs to review and improve the incident response process and outcomes. These activities include:

- Conducting a post-incident review or debriefing with the incident response team.
- Analyzing and evaluating the incident response process, performance, and results
- Identifying and documenting the strengths, weaknesses, opportunities, and threats of the incident response
- Developing and implementing the action plans and recommendations for improvement
- Updating and revising the incident response plan, policy, and procedures based on the lessons learned

Incident Response Tools

The incident response tools are the software and hardware that the incident response team uses to perform the incident response activities. The incident response tools may include:

- Network and system monitoring and analysis tools, such as Palo Alto Networks, Unifi.
- Malware analysis and removal tools, such as VirusTotal, Malwarebytes, or Microsoft defender
- Backup and recovery tools, such as NovaBackup or Synology
- Communication and collaboration tools, such as Microsoft Teams

Incident Response Communications

The incident response communications are the messages and information that the incident response team delivers to the internal and external parties during and after an incident. The incident response communications may include:

- Incident notification and escalation emails, phone calls, or text messages
- Incident status and resolution updates on the website, social media, or newsletter
- Incident report and summary on the incident details, actions, and results
- Incident feedback and survey on the incident response satisfaction and improvement

School District No. 50 Haida Gwaii

School District No. 50 (Haida Gwaii) recognizes the importance of technology and networking for enhancing learning and teaching, as well as for communicating and collaborating. The district is committed to providing safe, secure, and reliable technology and network services that comply with the relevant laws, standards, and policies.

The district also strives to promote digital citizenship and literacy among its students and staff, and to foster a positive and respectful online culture. The district is dedicated to ensuring that its technology and network are used in a responsible, ethical, and appropriate manner by all members of its community.