COMMITTEE REPORT OF THE
EDUCATION-POLICY COMMITTEE
School Board Office
December 6, 2022 – 6:00 p.m.

Present:
Allison Watson, Trustee (Committee Chair)
Cendra Beaton, Trustee (Committee Member)
Russ Chipps, Trustee (Committee Member)
Francesca Lee, STA
Lou Leslie, CUPE
Georgette Walker, SPVPA
Joanna Verano, SPEAC
Scott Stinson, Superintendent/CEO
Monica Braniff, Associate Superintendent
Dave Strange, Associate Superintendent
Paul Block, Associate Superintendent

Guests: Farzaan Nusserwanji -Chief Information Officer/Exec. Dir. Info Technology, Jim Lamond – District Principal – Pathways & Choice, Nicole Wallace, Dante Di Ponio and Brian Hotovy

1. **CALL TO ORDER AND ACKNOWLEDGMENT OF FIRST NATIONS TERRITORIES**
We are honoured to be meeting on the traditional territories of the Coast Salish: T'Sou-ke Nation and Sc'ianew Nation and Nuu-chah-nulth: Pacheedaht Nation. We also recognize some of our schools reside on the traditional territory of the Esquimalt Nation and Songhees Nation.

2. **Opening Remarks from Chair, Allison Watson**
Chair Allison Watson introduced members and welcomed everyone to the meeting.

3. **COMMITTEE REPORT** of Nov. 8, 2022 Education-Policy Committee meeting
The committee report for the Nov. 8, 2022 Education-Policy Committee meeting was reviewed by the committee. No errors or omissions were noted.

4. **BAA COURSE PROPOSALS**
There are no BAA course proposals for this meeting.

5. **REVIEW OF POLICIES/REGULATIONS**
   a. <u>Draft New Regulations F-325 "Cyber Risk and Security"</u> – Farzaan Nusserwanji
   Mr. Nusserwanji addressed previous concerns and feedback in tonight's Information Note. Appreciation was given to Mr. Nusserwanji for the detail and responsiveness in incorporating the committee's suggestions into the regulations.

Recommendation:
That the Board of Education for School District #62 (Sooke) receive the revised Administrative Regulations to accompany Policy F-325 “Cyber Risk and Security”.

6. **NEW BUSINESS**

a. Update – Student & Family Affordability Fund – Dave Strange
Mr. Strange highlighted areas that are currently being actioned in the District. SD62 is well into the implementation stage at both the District and school levels. Fee refunds are underway at the middle and secondary schools, and a tremendous effort has been made at all schools for innovative and thoughtful responses. There has been heartfelt thank you and appreciation from families for these efforts. Funds have also been transferred to community agencies as per the community agreements. Mr. Strange noted that one community agency, Thrive Social Services, voted to match District funding in support of students and families. Superintendent Stinson acknowledged the work of Mr. Strange and the team in creating a response that reaches out to community and provides a breadth of opportunities for families. The Chair also acknowledged the significance of this work and its relation to the District’s Strategic Plan.

Presentation – Youth Work in Trades/Youth Train in Trades and TASK Program – Jim Lamond/Careers Dept. Staff
Mr. Lamond introduced members of the Careers team who were present at tonight’s meeting: Nicole Wallace, Dante Di Ponio, and Brian Hotovy. They showed a video clip “Welding Update Celebration for Royal Bay Secondary School”. This video highlighted the passion and pathways available for students in welding and exemplified the partnership between SD62 and community worksites. Mr. Lamond and team presented on the Career Education K-12 Roadmap with a focus on who students want to be, and not limiting them to the “what”. Further information was shared about the vision and programming opportunities that lie within Career Education, including a renewed focus at the K-8 level. Several students were highlighted and honoured for their exemplary work. Questions/comments shared about supporting gender equality and inclusivity through education, protocols, and increased opportunities for women in trades. Associate Superintendent Block and Chair Watson acknowledged District/school teams for the growth in programming opportunities and strong community partnerships.

7. **FOR INFORMATION**
Nothing noted.

8. **FOR FUTURE MEETINGS**
Nothing noted.

9. **ADJOURNMENT AND NEXT MEETING DATE**: January 3, 2023

School District #62 (Sooke)

CYBER RISK AND SECURITY	No.: F-325
	Effective: Revised: Reviewed: Sept. 6/22; Sept. 27/22; Nov. 8/22; Dec. 6/22; Dec. 13/22

ADMINISTRATIVE REGULATIONS

The following administrative regulations support and further define cyber risk and security in the Sooke School District and are provided within the Cyber Risk and Security Policy.

1. Application and Scope

All School District 62 staff, students and vendors employed under contract, who have any involvement with digital assets, are responsible for implementing this policy and its regulations and shall have the support of the School District 62 Board which has approved the policy. This policy and its regulations cover digital assets and initiatives whether hosted by SD62 or a third party. Failure to comply with this policy may result in breaches of security, leading to the exposure of data of a confidential or sensitive nature.

2. Responsibilities pertaining to Cyber Risk and Security

The Board of Education's responsibilities:

- Board-level digital governance: setting policy, ensuring strategic alignment, risk assessment, resource management, and performance management of cyber risk and security efforts.
- Provide oversight, guidance, and direction on the cyber risk associated with digital initiatives
- Allocate funding for information and technology asset acquisition, currency, replacement, and operational support to ensure the protection of information technology assets and the provisioning of resources to ensure adequate security and privacy are maintained.
- Provide guidance on cyber risk tolerance and be ultimately accountable for cyber risk acceptance.

District Executive responsibilities:

- Provide direction and funding for information and technology asset acquisition, currency, replacement, and operational support to ensure the protection of information technology assets and the provisioning of resources to ensure adequate security and privacy are maintained.
- Provide oversight, guidance, and direction on the cyber risk associated with digital initiatives.
- Ensure each business or educational application, information and data system has an Accountable Executive who ensures cyber risk and security are assessed for the systems under their executive or departmental purview.
- The accountability to ensure the cyber risk assessment is conducted and associated recommendations implemented reside with the program/business owner.

Chief Information Officer responsibilities:

- Board's delegate for the Cyber risk assessment and security of digital assets, digital initiatives, systems infrastructure, and information contained therein, user access controls, and data recovery.
- Develop administrative procedures and standards consistent with this policy and its regulations.
- Provide strategic direction and recommendations related to the security and privacy of district digital solutions, information services, and technology to the Board and its committees.
- Managing information and technology legislation, including FOIPPA and the *Statistics Act*

- Collaborating with District Executive to develop and set policies, standards, processes, procedures, and guidelines for cyber risk and security.
- Ensure the implications of cyber risk and security are considered during strategic planning, staffing, budget, and risk management.
- Oversee and guide the security and privacy of digital transformation initiatives across the district
- Define the privacy and security posture including operational responsibility for the FOIPPA office
- Ensure Disaster Recovery plans are updated to reflect changes in assets and security configurations.
- Develop and deliver security and privacy training on an ongoing basis to new and existing employees

Human Resources along with Hiring Supervisors responsibilities:

- Prior to employment, employee and contractor security screening is completed, and employees and contractors are informed about information security policies, regulations, procedures and associated roles and responsibilities
- Reference and criminal records checks are completed prior to hiring or engagement.
- Responsibilities for information and systems security documented in the Acceptable Use Policy are signed off upon hire.
- Supporting management with determining the appropriate course of action in response to identified abuse of information and technology assets.
- Security breaches or policy violations that have been reported are investigated, and action is taken where warranted.
- Ensuring that a process is in place for the departure of employees, consultants, contractors, or temporary agency staff in relation to the retrieval of assets and reminding employees of their ongoing confidentiality responsibilities.
- If assets are not returned, follow up to attempt retrieval or seek additional remedies.
- Contractor responsibilities for information security are identified in contractual agreements.
- Ensuring all new and existing employees are trained on Security and Privacy on an ongoing basis.

Finance/Accounts Payable/Procurement responsibilities:

- Ensure the Chief Information Officer has been consulted during procurement and receives reports of all hardware, software, and cloud-based services to assess compliance with this policy and its regulations.
- Confirm risks related to external party access to information and information systems are assessed before accepting any acquisition of third-party software or cloud-based services
- Ensure the risks of external party access to information and information systems are identified, assessed, mitigated, and managed
- Confirm security controls, service definitions, and delivery levels are identified and included in agreements with external parties before using external information and technology services

Director, Facilities responsibilities:

- Developing and implementing the Physical and Environmental Security Program in consultation with the Chief Information Officer.

Internal Audit responsibilities:

- Conduct periodic reviews of processes, controls, and compliance with this policy and its regulations.

Department/Site Leadership responsibilities:

- Managing the use of the assets by employees at their site or within their site or department.
- Determining access levels and ensuring all staff in their area use IT assets responsibly.
- Monitoring compliance with this policy.

- Retrieving assets from departing employees, consultants, contractors, or temporary agency staff.
- Informing staff of their information security responsibilities and providing guidelines that clearly define how these security controls are managed.
- Notifying Information Technology of systems access requirements, changes to access requirements and removal of access when it is no longer required.
- Ensuring all privileged identities are tracked and recorded with the IT department.
- Promoting a *culture* of security, creating an appropriate level of awareness of security controls among staff, relevant to their roles and responsibilities, and an appropriate level of skills to comply with these security controls.
- Creating awareness of new or updated security requirements and monitoring adherence to the organization’s security policies.
- Reporting suspected security and privacy incidents that affect their area of responsibility to the CIO.
- Managing the response to security and privacy incidents that affect their areas of responsibility based on guidance from the CIO.

Staff responsibilities:

- Complying with School District 62 security policies, controls, standards, and procedures, and any department or school-specific security practices.
- Familiarizing themselves with security policies and reviewing them.
- Reporting suspected security and privacy incidents to their Supervisor.
- Returning technology assets when leaving the organization.
- Notifying the IT department of any loss or damage to assets.

Caregivers and Student responsibilities:

- Complying with School District 62 security policies, controls, standards, and procedures, and any school-specific security practices.
- Ensuring consent is provided for use of digital tools, software and cloud-based services
- Reporting suspected security and privacy incidents to their teacher and/or school administrators

3. Digital Asset Management

Information and information systems constitute valuable School District 62 resources. Digital asset management identifies what assets to protect, how to protect them, and how much protection is adequate.

Identification of Digital Assets

School District 62 departments and schools must identify and maintain an inventory of assets under their control including:

- Hardware
- Software
- Digital services including communications and cloud-based services.
- Digital information and data assets including student and staff records, database and data files, contracts and agreements, system documentation, research information, reports, user manuals, operational or support procedures, continuity plans and archived information.

Documenting and Maintaining Asset Inventories

School District 62 will establish and maintain an IT Asset Management program, create and maintain an inventory of important assets associated with information systems, and establish asset currency and lifecycle plans. The loss, theft or misappropriation of assets must be reported immediately to the IT Service Desk. Where the loss, theft or misappropriation involves information the Incident Response Plan will be initiated.

The IT Asset Management program must include:

Hardware Assets

- Hardware components shall be subject to full lifecycle management from acquisition to disposal, including hardware acquired but not implemented, hardware in storage or retired hardware.
- All hardware including servers and end-user computing devices must be refreshed with a currency cycle of no more than 4 years or the useful life of the device (as per support policies from the manufacturer) to ensure security updates, fixes, and patches can be applied and maintained.
- All hardware items, excluding low-value assets such as mouse devices, shall be uniquely named with an asset number and labelled. Vendor decals, stickers and other serial number identifiers should not be removed. Serial numbers and model numbers shall be recorded and tracked.
- IT Operations shall periodically confirm physical inventory via automated discovery tools and reconcile and document any discrepancies.
- All allocations, transfers, returns and disposals shall be tracked and documented except for low-value assets such as mouse devices.
- Lost assets shall be reported and investigated for a potential data breach.
- Service Request processes shall be used for replacements and upgrades.
- At end-of-life hardware assets will be logged and disposed of securely to protect School District 62 information.
- All student devices must be maintained at a security patch level that ensures adequate protection.
- All hardware assets including the operating system and installed software must be patched and upgraded to no more than 2 patch levels behind the latest release.
- All critical production hardware assets shall be supported by warranty or other maintenance agreements and shall be replaced before the expiry of support agreements.
- A process for recovery of hardware after notification of staff or contractor departures shall be in place.
- Hardware configurations shall be managed through configuration management processes and documented.
- Disaster Recovery plans shall be updated to reflect changes in assets and configurations.

Software Assets include digital communications and cloud-based services that are not hosted on-premise

- Disaster Recovery plans shall be updated to reflect changes in assets and configurations.
- All software licensing agreements and compliance shall be actively managed.
- All software installed on School District 62 hardware is to be appropriately licensed.
- All educational software must be reviewed for conformance with curricular, inclusion and diversity objectives and for the protection of student privacy, student records management and information protection compliance.
- All non-standard software implementations shall be managed and documented through an exception process.
- All software assets including the operating system and installed software must be patched and upgraded to no more than 2 patch levels behind the latest release.
- Variations in versions of software shall be minimized.
- Installed software versions shall be supported by vendors with patches available to address vulnerabilities.
- All digital communications and cloud-based services will be governed by the third-party vendor management framework under IT oversight.

Information and Data Assets

- Data will be treated as an asset and protected as such.
- The goals of data security include purpose limitation, fairness, lawfulness, transparency, data minimization, storage limitation, accuracy, confidentiality, integrity and accountability
- Every reasonable step must be taken to ensure that inaccurate personal data are erased or rectified without delay.
- Data (student, staff, financial statements, contracts, etc.) will be protected from unauthorized access and modification.
- Data shall be backed up regularly and disaster preparedness and recovery plans will be developed to protect and recover data from outages due to system outages or security breaches such as ransomware.
- Data classification, data standards, and data definitions shall be established to ensure the consistency of the information being shared. (Refer to section: **Data and Information Classification and Retention**)
- Every data source or application system will have a defined responsible steward who will act to ensure data security, data quality, availability, accuracy and transparency following the security policies, regulations and standards
- Integration and automation of data flow between different systems shall be securely implemented.

4. Human Resources role in Cyber Security

The role of Human Resources in cyber security is to ensure that employees, external consultants, and contractors accessing School District 62 information and information systems have been screened, understand, and accept their responsibilities for security, receive security training and that their access to information and systems is securely managed throughout their affiliation with the School District.

- Prior to employment, employee and contractor security screening is completed, and employees and contractors are informed about information security policies, regulations, procedures and associated roles and responsibilities
- Reference and criminal records checks are completed prior to hiring or engagement.
- Responsibilities for information and systems security documented in the Acceptable Use Policy are signed off upon hire.
- Supporting management with determining the appropriate course of action in response to identified abuse of information and technology assets.
- Security breaches or policy violations that have been reported are investigated, and action is taken where warranted.
- Ensuring that a process is in place for the departure of employees, consultants, contractors, or temporary agency staff in relation to the retrieval of assets and reminding employees of their ongoing confidentiality responsibilities.
- Ensuring School District 62 assets are returned on termination of employment unless other arrangements are made in advance and all School District 62 information and documents have been removed.
- If assets are not returned, follow up to attempt retrieval or seek additional remedies.
- Contractor responsibilities for information security are identified in contractual agreements.
- Ensuring all new and existing employees are trained on Security and Privacy on an ongoing basis.
- Ensuring access rights to information systems are terminated on termination of employment. Any school district data associated with the account access will be made available to the supervisor.

5. Physical and Environmental Security

IT equipment must be protected to reduce the risks of unauthorized access, environmental threats, and hazards. Physical and environmental security ensures that School District 62 has a risk-based physical and environmental security framework to govern the design, implementation and management of facility security and access to sites and facilities.

Physical Security

Physical security refers to the measures designed to prevent unauthorized physical access to equipment, facilities, material, information, and documents, and to safeguard them against espionage, sabotage, damage, tampering, theft, and other covert or overt acts. SD62 will design, document and implement security controls for a facility based on an assessment of security risks to the facility and establish appropriate entry controls to restrict access to secure areas and prevent unauthorized physical access to district information and devices.

Environmental Security

SD62 will ensure environmental security design to address the requirements to provide appropriate temperature and humidity controls, dust control, fire protection, power, and natural disaster protection necessary to ensure the continuity of operations for the School District's facilities and equipment. Digital assets in schools such as servers, switches and network devices should be adequately ventilated and free from obstruction to ensure the stability and security of systems.

6. Network Security Controls

A range of controls must be implemented to achieve and maintain security and reliable access and performance within School District 62 network.

Network infrastructure security controls and security management systems must be implemented for networks to ensure the protection of information and attached information systems.

School District 62 must protect network-related assets including:

- Information in transit.
- Stored information (e.g., cached content, temporary files).
- Network infrastructure.
- Network configuration information, including device configuration, access control definitions, routing information, passwords, and cryptographic keys.
- Network management information.
- Network pathways and routes and bandwidth resources.
- Network security boundaries and perimeters.
- Information system interfaces to networks.

Employees, contractors, and external consultants must not store School District 62 information on non-School District 62 owned and managed computing devices. Non-School District 62-owned computing devices must follow the BYOD expectations when connecting to the School District 62 network.

Inappropriate Use

Any device found to be in violation of this regulation or found to be causing problems that may impair or disable the network in any way, may be subject to immediate disconnection from the network.

Attempting to circumvent security or administrative access controls for information resources is a violation of this regulation. Assisting someone else or requesting someone else to circumvent security or administrative access controls is also a violation of this regulation.

Network usage judged inappropriate includes, but is not limited to:

- Establishing unauthorized network devices, including a router, gateway, or remote access service such as wireless.
- Using network services or devices to conduct any unlawful activity.
- Using network services that, while legal, would reasonably be considered unacceptable to School District 62's practices.
- Engaging in network packet sniffing other than for network problem diagnosis.

Configuration Control

To maintain the integrity of networks, all changes to network and server configuration must be managed and controlled such as configuration data, access control definitions, routing information and passwords.

Network device configuration data must be protected from unauthorized access, modification, misuse, or loss using controls such as:

- Encryption
- DMZ and network segregation
- Access controls and multi-factor authentication
- Monitoring of access
- Configuration change logs
- Configuration baselines protected by cryptographic checksums
- Regular backups

Firewall reviews must be performed at least annually by the information technology department and after any significant changes to ensure those configuration baselines reflect actual device configuration.

Secured path for Confidential/Sensitive information

Secured paths must be used for transmission of personally identifiable and sensitive/confidential information transmission using controls such as:

- Data, message, or session encryption
- Encrypted email, secure file transfer systems

Wireless Local Area Networking

Wireless Local Area Networks must utilize the controls specified below:

- Strong link layer encryption, such as Wi-Fi Protected Access.
- User and device network access is controlled by School District 62 authentication services.
- The use of strong, frequently changed, automatically expiring encryption keys and passwords.
- Segregation of wireless networks from wired networks using filters, firewalls, or proxies.
- Port-based access control, for example, use of 802.1x technology.

Management of Removable Media

All removable computer media must be managed with controls appropriate for the sensitivity of the data contained in the media.

Use of Portable Storage Devices

The use of portable storage devices to store or transport information increases the risk of information compromise as these devices are easily lost, stolen or damaged, particularly when transported in public environments. Employees using portable storage devices must protect the information and information technology assets in their custody or control by ensuring it is physically secure.

7. Bring Your Own Device (BYOD)

School District 62 recognizes that users may choose to access SD62 District Technology Resources utilizing a personal electronic device including but not limited to computers, phones, tablets, cellular/mobile technology, internet of things (IoT), and artificial intelligence (AI) devices. Routers and wireless access points are not considered to be BYOD and are not permitted to be connected to the district's network.

By connecting to or using the District Technology Resources (e.g. Wifi network, information systems) through a personally owned device, to reduce risk and ensure security, users accept a loss of personal privacy.

The goal of BYOD security is to ensure that end users can safely and securely use district technology resources. The objective is not to patrol instead it is to protect.

District authorities reserve the right to audit the device and its network usage when necessary to mitigate cyber risk and ensure compliance with school and school district codes of conduct, policies, and guidelines.

Cyber Security audits and investigations are conducted on the express authority of the Superintendent of Schools.

- Under FOIPPA, if users have records on their personal devices (BYOD) SD62 authorities can request users to search those devices themselves.
- *Under FOIPPA,* failure to disclose any record or an attempt to alter a record is considered an offense under the act.
- SD62 authorities can search personal devices after informing the user and getting consent.
- SD62 authorities cannot search personal devices electronically without informing the user.
- Emergency situations, written police requests, and compelling health and safety (e.g. suicide or attack threats) are exceptions that may allow SD62 authorities to collect and disclose information after engaging legal advice.

The use of personally owned devices will follow the regulations outlined in Policy B-117 Acceptable Use of Technology.

8. Business Information Systems

Security controls must be implemented to mitigate the business and security risks associated with the interconnection of business information systems (e.g. including but not limited to HR, Finance, Facilities, Payroll, Transportation and Student Information systems).

System and Security management controls should be developed, documented, and implemented by the Accountable Executive and their staff to ensure:

- Duties and areas of responsibility are segregated to reduce opportunities for unauthorized modification or misuse of information systems.
- Acceptance criteria for new information systems, upgrades and new versions are established and suitable tests of the system are carried out before acceptance.
- Security review and acceptance criteria are included as part of the information system development and software acquisition process.

- Security awareness, prevention and detection controls are utilized to protect information systems against malicious code.
- Records are maintained of changes to published information (audit and change logs).
- Inappropriate release of sensitive or personal information is prevented.
- Monitoring is conducted for unauthorized changes.
- Unauthorized access to networks and information systems is prevented.
- All privileged identities are tracked and recorded with the IT department.
- Audit logs recording user activities, exceptions and information security events must be produced and stored to assist in access control monitoring and future investigations.
- Secure forms of data transmission are used (e.g. encrypted email) to transfer sensitive and personally identifiable data.
- HR, Payroll, Facilities, Transportation and Finance information systems are compliant with this policy and its regulations.
- Oversight assurance and periodic review of security controls by the IT department are undertaken.

Online Transaction Security

Information systems containing online transactions must have security controls commensurate with the value and classification of the information.
Security controls must be implemented to prevent incomplete transmission, miss-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication and replay. Security controls include:

- Validating and verifying user credentials.
- Using digital signatures.
- Multi-factor authentication.
- Using cryptography to protect data and information.
- Establishing secure communications protocols.
- Storing online transaction details on servers within the appropriate network security zone.

Publicly Available Information

Management must pre-authorize the publication of information on publicly available information systems and implement processes to prevent unauthorized modification.

Internet Site Security

The publication, modification, or removal of information on publicly available information systems must be approved by the staff member managing the website content. Staff who are website content managers are responsible for maintaining the accuracy and integrity of published information.

9. Access Control

Access restrictions protect organizations from security threats such as internal and external intrusions. The restrictions are guided by regulations that protect particular types of information (e.g. public, internal, confidential) and FOIPPA requirements. Mechanisms for access control include password management, user authentication and user permissions.

Access Control

Access to information systems and services must be consistent with business needs and be based on security requirements. All privileged accounts and identities must be tracked and recorded with the IT department.

Access controls should:

- Consider both physical and logical access to assets.

- Apply the “*need to know*” and “*least privilege*” principles.
- Set default access privileges to “deny-all” before granting access.
- Require access by unique user identifiers or system process identifiers to ensure that all accesses are auditable.
- Have permissions assigned to roles rather than individual user identifiers.
- Use encryption and multi-factor authentication

Access Management

There must be a formal user registration and de-registration process for granting access to all information systems in use within School District 62. It is each department’s responsibility to ensure that access controls are implemented for information systems within their management purview.

Password Management

The issuance of authentication credentials must be controlled through a formal management process. Individuals must be formally designated to have the authority to issue and reset passwords.

Review of Access Rights / Privileges

User access rights must be reviewed at regular intervals. A formal process must be implemented for the regular review of access rights. Privileged and Administrative accounts must be registered with IT and access logs reviewed regularly.

10. Cyber Risk Assessment

A cyber risk assessment will be performed at the start of all digital initiatives to ensure that cyber risk management controls are identified and considered at the start of the initiative and through the life cycle of service delivery.

The accountability to ensure the cyber risk assessment is performed remains with the program/business owner. The program/business owner will own the risks identified in the cyber risk assessment, and its disposition, and agree to establish completion dates for cyber risk management controls that are identified (ex. Consent process for students) as part of the cyber risk assessment.

The CIO or IT department representative reserve the right to identify and block hardware, software or a 3rd party cloud service from the network and notify the accountable executive if the risk is high, and/or if the program/business owner has not agreed to implement the appropriate cyber risk management controls within a reasonable timeframe.

11. Information Security and Privacy Breach Incident Management

School District 62 will establish procedures and processes so that employees, external consultants, and contractors understand their roles in reporting and mitigating security events.
Information security and privacy breach events and weaknesses must be immediately reported through appropriate management channels.

Staff must report suspected security and privacy incidents to their Supervisor.
Procedures to detect, respond and recover will be established to manage security incidents and breaches.

Under the amended FOIPPA legislation, it is now required that all public bodies such as SD62:

- Establish a Mandatory Privacy Management Program and ensure Mandatory Breach Reporting to the Office of Information Privacy Commissioner (OIPC).

- Conduct Privacy Impact Assessments on software and 3rd party services that the head of the public body must sign off on to ensure vendors have privacy and security breach management protocols in place.

SD62 will follow OIPC guidance on administrative, technical, and contractual controls and consideration of volume, sensitivity, harm, and foreseeability of risk.

SD62 will ensure all reasonable alternatives within Canada are considered prior to moving or storing any data that could be subject to a privacy breach outside of Canada.

12. Cyber Security Assessments and Vulnerability Scans

To ensure that School District 62 security posture is continuously informed and updated, management shall conduct periodic cyber security assessments against other school districts and industry standards such as NIST or COBIT.

Management will conduct periodic vulnerability scans including “ethical hacking” to determine vulnerabilities in the information systems and physical networks.

While reviewing and accepting results from these scans, SD62 will find an optimum balance between improving security opportunities and educational and administrative requirements within the financial and resource constraints of the district.

13. Data and Information Classification and Retention

School District 62 will establish a data classification system that identifies public, internal, and confidential information and will utilize appropriate access and transmission controls when sharing this data internally or externally. Techniques to secure data may include encrypted email and secure file transfer and storage protocols.

SD62 will establish clear data management, records management, retention, and storage policies in support of secured data access for software hosted on-premises or via 3rd party cloud service providers.

Records Management policies and retention schedules should cover staff personal records, school records, administrative records, human resources, and financial records.

All digital communications and cloud-based services will be governed by the third-party vendor management framework under IT oversight to ensure the privacy and protection of data and records management policies are followed.

Data and Information Classification Definitions

Classification	Definition
Public	• Any information that may or must be made available to the public, with no legal restriction on its access or use. • While little or no controls are required to protect the confidentiality of public data, basic security is required to ensure the integrity of district information.
Internal	• Any information that is produced only for use by members of the school district who have a legitimate purpose to access such data. • Internal data is designated by the data owner where appropriate. • Any information of a sensitive nature which is intended for limited internal use only (i.e. between specific individuals or groups of staff) • Access to limited data and information is provided by the owner(s) who created it.

	• Internal data is not intended to be shared with the public and should not be shared outside of the school district without the permission of the person or group that created the data. • Internal information requires a reasonable level of security controls with a varying degree of access control.
Confidential	• Any information protected by government legislation or contract. Example: Freedom of Information and Protection of Privacy Act (FOIPPA). • Any other information that is considered by the district as appropriate for confidential treatment. • Any information that if made available to unauthorized parties may adversely affect individuals or the school district. • Confidential information requires the highest level of security controls with varying degrees of access control. • Confidential data must be protected both when it is in use and when it is being stored or transported.

14. Mobile Computing

School District 62 will ensure appropriate controls are implemented to mitigate cyber risks associated with the use of portable devices including laptops, iPads, smartphones, etc.

Information protection

The use of portable devices must be managed and controlled by the Information Technology team to mitigate the inherent *risks* of portable devices using technologies such as Mobile Device Management and Encrypted Storage to ensure that SD62 administrators can monitor, track and erase data.

The use of devices such as laptops, and mobile devices (smartphones) to access, store, or process information increases the risk of information being compromised.

Users of mobile computing services must ensure that information and information technology assets in their custody or control are protected.

Definitions:

Accountable Executive/Program/Business Owner – a member of the District Executive who is the owner and/or sponsor of an SD62 digital initiative, software or 3rd party cloud service. Typically, accountable for overseeing district departments or schools.

Availability - Information or information systems being accessible and usable on demand to support business functions.

Bring Your Own Device (BYOD) - refers to personal district network or internet-connected devices (laptops, phones, tablets, etc.), internet of things (IoT) devices and artificial intelligence (AI) devices. Routers and wireless access points are not considered to be BYOD and are not permitted to be connected to the district's network.

Business Continuity Plans - contain the recovery procedures and strategies necessary to resume critical services and are activated when standard operational procedures and responses are overwhelmed by a disruptive event

Confidentiality - Information is not made available or disclosed to unauthorized individuals, entities, or processes. Control - any policies, processes, practices, or other actions that may be used to modify or manage information security risk.

Cryptography - the discipline which embodies principles, means and methods for the transformation of data to hide its information content, and prevent its undetected modification or prevent its unauthorized use.

Cyber Risk - a negative event caused by a threat or opportunity to exploit a weakness in underlying technology resources, processes, or people.

Cyber Risk Assessment - a process that assesses the cyber risks for a digital initiative in which recommendations are provided to manage such risks. This process is defined through Digital Governance.

Information and Data - include but is not limited to SD62 student records, employee records, confidential, personal, or professional information and communications, or any other electronically formatted information.

Device - An IT Resource that can connect (wired, wireless or cellular) to the government network, including but not limited to computers, laptops, tablets, smartphones, and cell phones.

Digital Asset - includes district technology resources and digital district learning resources, software information systems, 3rd party cloud services, information and data, and hardware technologies. Digital assets include but are not limited to computers, phones, tablets, cellular/mobile technology, applications, emails, servers, networks, internet services, internet access, information and data, websites and any other electronic or communication technology provided by the Sooke School District or third party that exists today or may be developed in the future.

Digital Governance - a subset of board governance and has five primary objectives:

- Deliver value by ensuring quality IT (Information & Technology) services to facilitate innovation in delivering education and improving the efficiency of business processes.
- Create alignment with and support integration of business, educational and administrative outcomes.
- Ensure we are optimizing the use of digital resources and promoting digital literacy.
- Monitoring the performance and value derived from digital initiatives and investments.
- Mitigating IT risks.

Digital Initiative - any School District 62-sponsored project or initiative that involves the use of new (procured or developed) and/or enhancements to existing information and technology.

District Technology Resources include - Access to the District’s wired and wireless network from any location, such as schools, workplaces, home or other offsite locations, Board of Education-provisioned hardware, such as desktop computers, laptop computers, tablets and printers (and including removable and/or external storage devices), Access to the Board of Education’s technical support services, and Board of Education-provisioned software and applications, including cloud-based resources.

Information System - A system (including people, machines, methods of organization, and procedures) that provides input, storage, processing, communications, output, and control functions in relation to information and data. Normally used to describe computerized systems, including data processing facilities, database administration, hardware, and software that contain machine-readable records. A collection of manual and automated components that manages a specific data set or information resource.

Integrity - the characteristic of information is accurate and complete and the preservation of accuracy and completeness by protecting the information from unauthorized, unanticipated, or unintentional modification.

Least Privilege - a principle requiring that each subject in a system be granted the most restrictive set of privileges (lowest clearance) needed to perform their employment duties. The application of this principle limits the damage that can result from accidents, errors, or unauthorized use.

Need-to-know - a principle where access is restricted to authorized employees that require it to carry out their work. Employees are not entitled to access merely because of status, rank, or office.

Packet sniffing - a technique whereby packet data flowing across the network is detected and observed.

Office of the Information Privacy Commissioner (OIPC) - The Office of the Information and Privacy Commissioner provides independent oversight and enforcement of BC's access and privacy laws, including the Freedom of Information and Protection of Privacy Act (FIPPA), which applies to over 2,900 "public bodies" including ministries, local governments, schools, crown corporations, hospitals, municipal police forces.

Security Screening - verification of facts about individuals related to their identity, professional credentials, previous employment, education, and skills.

Threat – a potential cause of an unwanted incident, which may result in harm to a system or organization.

User - any individual who accesses SD62 IT Resources through any electronic or communication activity with any device (whether such device is personally owned or provided by the district) and regardless of the user’s physical location. Users include but are not limited to students, employees, contractors, trustees, parents, guardians, volunteers, and guests.

Vulnerability - weakness of an asset or control that can be exploited by one or more threats