COMMITTEE REPORT OF THE
EDUCATION-POLICY COMMITTEE via MS Teams
School Board Office
September 6, 2022 – 6:00 p.m.

Present: Allison Watson, Trustee (Committee Chair)
Margot Swinburnson, Trustee (Committee Member)
Dianna Seaton, Trustee (Committee Member)
Christina Kempenaar, STA
Lou Leslie, CUPE
Sandra Arnold, SPEAC
Shannon Miller, SPVPA
Scott Stinson, Superintendent/CEO
Monica Braniff, Associate Superintendent
Paul Block, Associate Superintendent
Dave Strange, Associate Superintendent

Guest: Farzaan Nusserwanji

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.

1. **Opening Remarks from Chair, Allison Watson**

2. **COMMITTEE REPORT** of June 9, 2022 Education Standing Committee meeting.
The committee report for the June 9, 2022 Education-Policy Committee meeting was reviewed by the committee. No errors or omissions were noted.

3. **BAA COURSE PROPOSALS**
There were no BAA course proposals for this meeting.

4. **REVIEW OF POLICIES/REGULATIONS**
   a. Draft New Policy and Regulations F-325 - "Cyber Risk and Security" – Farzaan Nusserwanji
   A detailed overview of the draft policy and regulations was given by Farzaan Nusserwanji, Chief Information Officer and Executive Director of IT.

   Questions and discussion followed and included inquiries as to training of staff and students, reporting processes, privacy of staff and student personal devices used in school and work setting,

security screening, comparable policies from other school districts, implementation costs, visitor and PAC member access, etc. Feedback was given and recorded for possible revision and updates to the Policy and Regulations.

Recommendation
That the Board of Education for School District #62 (Sooke) give Notice of Motion to draft new Policy and Regulations F-325 "Cyber Risk and Security" and that draft revisions come back to the Education Policy Committee prior to final ratification by the Board.

6. **NEW BUSINESS**

a. Outdoor Learning Update – Scott Stinson
The Superintendent provided an update on outdoor learning spaces, programs and initiatives in the district. Questions and discussion followed. A key point made was that while the district has many initiatives in this area, further clarity is needed relative to the original Board motion to "understand the resources required to support, develop and implement increased outdoor learning opportunities".

b. Ministry of Education – Student and Family Affordability Fund – Scott Stinson
The Superintendent provided information on the newly announced "Student and Family Affordability Fund" as well as an update on the initial action and planning being done in the district to utilize the funding. Associate Superintendent Dave Strange will be leading the work in this area and provided additional information. Questions and discussion followed.

7. **FOR INFORMATION**
a. Research Project Approval – no project approvals at this time.

8. **FOR FUTURE MEETINGS**

9. **ADJOURNMENT AND NEXT MEETING DATE**: October 4, 2022

School District #62 (Sooke)

CYBER RISK AND SECURITY	No.: F-325
	Effective: Revised: Reviewed: Sept. 6/22

SCHOOL BOARD POLICY

The purpose of this policy is to protect the information and technology assets of School District 62 from all cyber risks, whether internal or external, deliberate, or accidental. It is the policy of School District 62 to provide secure access to information and technology for use by students, staff and other users in a manner that complies with related provincial, district, and school policies and guidelines.

Principles that guide the security of Information and Technology (Digital Assets) at SD62:

- The Board delegates responsibility for the Cyber Risk Assessment and Security of digital assets, digital initiatives, systems infrastructure, and information contained therein, user access controls and data recovery to the Chief Information Officer (CIO).
- The CIO shall develop the appropriate administrative regulations and standards consistent with this policy. The responsibility for implementing this policy, its regulations and associated standards are shared with the Accountable Executive for the systems within their Executive and departmental or site purview.
- Information systems, data, and technologies are defined and managed as digital assets by the School District and are understood, provided, maintained, and protected as such.
- Understanding that there is no such thing as absolute security – Cyber Risk protection is balanced with utility.
- The primary goal of cybersecurity is to maintain Confidentiality, Integrity, and Availability of information.
- The three types of security controls are Preventative, Detective, and Responsive.
- People, Processes, and Technology are all needed to adequately secure an information system or facility.
- Information is not disclosed to or modified by unauthorized persons through deliberate or careless action.
- The principle of least access privilege is applied. Availability of information is to authorized users only.
- Regulatory and legislative requirements (e.g. FOIPPA, *Statistics Act*) are met.
- Digital Governance practices are established and followed.
- Business continuity plans to respond to cyber security events are produced, maintained, and tested.
- Information security training is given to all employees.
- All breaches of information security and suspected weaknesses are reported and investigated.
- All exceptions to the policy require Executive approval.

All School District 62 staff and vendors employed under contract, who have any involvement with digital assets, are responsible for implementing this policy and shall have the support of the School District 62 Board of Education who have approved the policy. Failure to comply with this policy may result in breaches of security, leading to the exposure of data of a confidential or sensitive nature.

Definitions:

Accountable Executive/Program/Business Owner is the owner and/or sponsor of an SD62 digital initiative, software or 3rd party Cloud Service, e.g. a district department or representative.

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

Business Continuity Plans - contains 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 is a negative event caused by a threat or opportunity to exploit a weakness in underlying technology resources, processes, or people.

Cyber Risk Assessment is 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 software information systems, 3rd party cloud services, data, and hardware technologies including but is not limited to computers, phones, tablets, cellular/mobile technology, applications, emails, servers, networks, internet services, internet access, 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 regardless of whether or not it may be used as a stand-alone device.

Digital Governance is 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 is 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.

Information System - A system (including people, machines, methods of organization, and procedures) which 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 which 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 being 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.

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 is 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.

Related Policies and References:

- Policy B-115 – Learning Resources
- Policy B-117 – Acceptable Use of Technology
- Policy F-200 – Purchasing
- FOIPPA – *Freedom of Information Privacy Protection Act*
- National Institute of Standards and Technology (NIST) – Cyber Security Framework
- Information Systems Audit and Control Association (ISACA) - COBIT Framework
- ISO 38500 / 27001
- BC Core Policy and Procedures Manual
- BC Government Office of CIO – Information Security Policy

School District #62 (Sooke)

CYBER RISK AND SECURITY	No.: F-325
	Effective: Revised: Reviewed: Sept. 6/22

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

These regulations apply to all SD62 staff, including consultants, contractors or other persons who wish to initiate a digital initiative whether hosted by SD62 or third party. These regulations also apply to all of the Board's digital initiatives and consumers of information, data and technology assets.

2. Responsibilities

Board of Education is responsible for:

- Board level Digital Governance: setting policy, ensure strategic alignment, value delivery, risk management, resource management, performance management.
- Provide oversight, guidance, and direction on digital initiatives.
- Providing support and funding for information and technology asset acquisition, currency, replacement, and operational support.

District Executive is responsible for:

- Providing support and funding for information and technology asset acquisition, currency, replacement, and operational support.
- Provide oversight, guidance, and direction on digital initiatives and priorities.
- Each Business or Educational Application, Information and Data system shall have an accountable executive that works with the CIO to ensure cybersecurity and risk management are assessed and implemented for the systems under their executive or departmental purview.

Chief Information Officer is responsible for:

- Providing strategic direction and recommendations related to 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 leadership to develop and set policies, standards, processes, procedures, and guidelines.
- Supporting district operations and assessing the implications of Cyber Risk and Security in strategic planning, staffing, budget, and risk management.
- Oversee and guide digital transformation initiatives across the district.
- Defining the privacy and security posture including operational responsibility for the FOIPPA office.
- Ensuring Disaster Recovery plans are updated to reflect changes in assets and configurations.

Human Resources along with Hiring Supervisors are responsible for:

- Prior to employment, employee security screening is completed, and employees are informed about information security policies and procedures, information security roles and responsibilities.
- Supporting management with determining the appropriate course of action, including disciplinary action in response to identified abuse of information and technology assets.
- 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.

Finance/Accounts Payable/Procurement is responsible for:

- Ensuring the Chief Information Officer has approved the procurement and receives reports of all hardware, software, and cloud-based services to assess compliance with this policy and its regulations.
- Ensure business requirements and associated risks related to external party access to information and information systems are assessed prior to 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.
- Ensure security controls, service definitions, and delivery levels are identified and included in agreements with external parties prior to using external information and technology services.

Director, Facilities is responsible for:

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

Internal Audit is responsible for:

- Conducting periodic reviews of processes, controls, and compliance of this policy and its regulations.
- Monitoring resolution of issues.

Department/Site Leadership is responsible for:

- Managing use of the assets by employees at their site or within their site or department.
- 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.
- 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 security policies of the organization.
- Reporting and managing security incidents that affect their area of responsibility.

Staff are responsible for:

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

3. Asset Management

Information and information systems constitute valuable School District 62 resources. Asset management identifies the rules of acceptable use and the rules for protection: what assets to protect, who protects them, and how much protection is adequate.

Identification of assets

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

- Hardware.
- Software.
- 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 must 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.
- All hardware items, excluding low value asset 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 with the exception of low value assets such as mouse devices.
- Lost assets shall be reported and investigated for potential data breach.
- Service Request processes shall be used for replacements and upgrades, where applicable.
- At end-of-life, hardware assets will be logged and disposed of in a secure manner to protect School District 62 information.
- All student devices must be maintained at a district specified ratio and be at a security patch levels that ensures adequate protection.
- All hardware assets, including 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 agreement and shall be replaced before 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 protection of student privacy and information protection.
- All non-standard software implementations shall be managed and documented through an exception process.
- All software assets, including 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, and transparency, data minimization, storage limitation, accuracy, confidentiality, integrity and accountability
- Data managed in the district will be accurate and, where necessary, kept up to date.
- Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, 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 consistency of 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, and accuracy and transparency in accordance with the security policies, regulations and standards.
- Where possible, data integration and automation of data flows between different systems shall be securely implemented.

4. Human Resources role in Information and Technology Security

The role of Human Resources in information and Technology 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 the period of their affiliation with the School District.

These are the information security regulations that apply to employees, external consultants, and contractors that have an employment relationship with School District 62.

- Reference, credit, and criminal records checks must be completed prior to hire or engagement.
- Responsibilities for information and systems security documented in the Acceptable Use Policy must be signed off upon hire.
- Security breaches or policy violations must be reported and investigated, and appropriate disciplinary action taken where warranted.
- All School District 62 assets must be returned on termination of employment unless other arrangements are made in advance and all School District 62 information and documents have been removed.
- Access rights to information systems must be terminated on termination of employment.

5. Physical and Environmental Security

IT equipment must be protected to reduce the risks from 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

Environmental Security addresses 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.

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 consider network-related assets which require protection 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.
- Network resources such as bandwidth.
- 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, is 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, changes to network device 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.
- 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 and after any significant changes to ensure that configuration baselines reflect actual device configuration.

Secured path

Where required information must only be transmitted using a secured path.

Secured paths for information transmission must use controls such as:

- Data, message, or session encryption.
- Encrypted email, secure file transfer systems.
- Systems to detect tampering.

Wireless Local Area Networking

Wireless Local Area Networks must utilize the controls specified by the Information Security Officer and must include:

- Strong link layer encryption, such as Wi-Fi Protected Access.
- User and device network access 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 on the media.

Use of portable storage devices

The use of portable storage devices to store or transport information increases the risk of information compromise. Portable storage devices are typically small, portable and 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 encrypted and physically secure

7. Bring Your Own Device (BYOD)

School District 62 recognizes that users may choose to access SD62 Information and Technology Resources utilizing a personal electronic device including but not limited to computers, phones, tablets, and cellular/mobile technology.

By connecting to or using the district's Information and Technology Resources (ex. Wi-Fi network) through a personally owned device, users accept a loss of personal privacy. District authorities reserve the right to inspect the device and its contents and monitor network usage to mitigate cyber risk and ensure compliance with school and school district codes of conduct, policies, and guidelines.

The use of personally owned devices will follow the regulations of 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. HR, Finance, Payroll, and Student Information systems).

System and Security management controls should be developed, documented, and implemented 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 prior to 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).
- Maintain the integrity of published information.
- Prevent the inappropriate release of sensitive or personal information.
- Monitor for unauthorized changes.
- Prevent unauthorized access to networks and information systems.

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 on-line 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 appropriate website manager. Website managers are responsible for maintaining the accuracy and integrity of the published information.

Audit Logging

Audit logs recording user activities, exceptions and information security events must be produced and kept to assist in access control monitoring and future investigations.

9. Access Control

Access restrictions protect organizations from security threats such as internal and external intrusions. The restrictions are guided by regulations that protects particular types of information (e.g., personal, sensitive, 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.

Access control 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" prior to 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.

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.

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 reserves the right to reject any digital initiative 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. Employees must immediately report all suspected or actual information security events to the IT Team and requirements for handling security events must be included in contracts and service agreements.

Procedures to detect, respond and recover will be established to manage security incidents and breaches.

The types, volumes and costs of information security incidents must be quantified and monitored.

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 IT Security opportunities and IT 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.

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

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 is 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 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, mobile devices (smart phones) 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.

POLICY AND REGULATIONS ADOPTION

School District #62 (Sooke)

September 27, 2022

Draft new Policy and Regulations F-325 ”Cyber Risk and Security” are now ready for Notice of Motion.

NOTICE OF MOTION:

That the Board of Education of School District 62 (Sooke) give Notice of Motion to draft new Policy and Regulations F-325 “Cyber Risk and Security”.