	DATE	DESIGNATION	NAME	SIGNATURE
DEVELOPED/UPDATED BY:	10/2025	PRINCIPAL	OLESIA POPENKOVA	
APPROVED BY:	10/2025	PRINCIPAL	OLESIA POPENKOVA	
APPROVED BY:	10/2025	CHAIRMAN OF THE BOARD	DR. LOUAY JEROUDI	
DATE OF REVIEW				

Introduction

The Russian School of Abu Dhabi (RSAD) is committed to establish a robust secure digital infrastructure and ensure the relevant cybersecurity controls.

This policy outlines principles, standards and rules for cybersecurity, school data protection and external providers.

Purpose

The purpose of this policy is to:

1. establish a robust secure digital infrastructure and ensure the relevant cybersecurity controls;
2. ensure that personal information is dealt with correctly and securely;
3. develop response and business continuity plans to guide staff in the event of a cybersecurity incident;
4. to develop a risk assessment framework for selecting external IT service providers and products related to the school network, system, and infrastructure, including learning application providers and open-source applications.

Data and cybersecurity Infrastructure

1. **Access control**
   - All school software, network, and digital devices must be used only for educational and administrative purposes.
   - The creation and management of school accounts is carried out by the IT department.
   - If user has forgotten or lost his password, he must contact the IT Department to obtain a new password.
   - Access to school educational resources is provided through the school account.
   - All school accounts are divided by roles into administrators (superuser), staff and students. Each role has a different access right to resources.
   - The external platform (such as Apple School Management, Google Workspase, MDM platforms etc.) and critical services that have a two-factor identification must only be used with it.
2. **Data encryption**
   - For data transmitted to internal and external recipients, use only encrypted channels, provided by the school.
   - Data must only be stored on devices with a school account.
   - Passwords for the school account must be kept confidential and should not be shared with anyone, including friends, classmates, or unauthorized staff.
     Placing data on any public network resources is strictly prohibited.
3. **Network security**
   - A firewall must be used to protect the school network against unauthorized access and to provide granular visibility on user browsing activity. The IT department is responsible for updating it regularly.
   - • To enable web filtering of content in use and the ability to block inappropriate content, school devices must be enrolled in mobile device management (MDM) software that includes this feature.
   - The MDM profiles establish unified security edge architecture for all internet browsing.
   - All school Windows and Android devices must use antivirus software. These devices must be able to be remotely managed.
   - IT department must regularly monitor and audit network traffic for unusual patterns.
4. **Endpoint protection**
   - All school Windows and Android devices must use antivirus software.
   - All school devices must have the latest software updates, including antivirus and operating system updates.
5. **Data backup and recovery**
   - Automated backups of critical data will be performed daily and stored securely in off-site locations.
   - In case of a security incident user must follow the next action plan:

1. Immediately report any suspected security incident to IT personnel.
2. Isolate affected devices from the network to prevent further damage.
3. Disable compromised accounts and change login credentials as needed.

- In case of detecting of suspicious activities or security breaches the IT department must:
  1. Isolate affected devices from the network to prevent further damage.
  2. Notify all relevant stakeholders about the incident and initial response actions.
  3. Identify the nature, scope, and cause of the incident.
  4. Document affected systems, data, and users.
  5. Determine if personal or sensitive data has been compromised.
  6. Restore affected systems using the latest secure backup.
  7. Apply necessary security patches and software updates.
  8. Reset passwords for impacted accounts and implement additional security measures.
  9. Record details of the incident, including cause, response, and resolution.
  10. Report findings to school administration and external authorities if necessary.

6. **Data security**
   - All data on the school network should be separated by user roles. Based on these roles, access control policies must be established on the data to determine who can view, edit, and share the data.
   - The sensitive data must be encrypted at rest (stored files) and in transit (emails, uploads) and enable TLS/SSL encryption for secure network communications.
   - School devices must use BitLocker (Windows) or FileVault (Mac) for full disk encryption.
7. **Security awareness training**
   - The IT department should conduct regular training sessions for staff and students to raise awareness about cybersecurity threats and best practices.
   - This training must be conducted at least once every 4 months.
8. **Physical security**
   - School physical servers, networking and other critical equipment should be installed in separate rooms.
   - All these rooms must have a key card lock.
   - Access to these areas is restricted to authorized personnel only according to the School Access card policy.
9. **Regulatory compliance**
   - All software and hardware must comply with local and international data protection regulations and standards.
10. **Monitoring and logging**
    - The school firewall must have monitoring systems to detect and respond to security incidents in real time.
    - All incidents must be logged into the firewall system.
    - The IT department must record all incidents.
11. **Secure software development**
    - The users must follow secure coding practice when developing software.
    - The IT department must regularly update and patch software to address vulnerabilities.
12. **Cloud security**
    - If using cloud services, ensure the selected providers adhere to stringent security standards.
    - The devices must implement proper configuration and control of access to cloud resources.

- Cloud Services – Software as a Service (SaaS) must integrate with school identity services where possible, with Saas Security Posture Management capabilities.

13. **Collaboration security**
    - The school must provide secure communication and collaboration platforms to protect sensitive educational information shared between students and staff.
14. **Third-party security**
    - All external IT service providers and products related to the school network, system and infrastructure, including providers of educational applications and open-source applications, must comply with the following requirements:
        1. Compatibility with existing school systems**.**
        2. Secure management data.
        3. Compliance with cybersecurity standards and frameworks.
        4. Security against cyber threats.
        5. Service delivery and backup/ recovery provisions.
        6. Reputation and financial stability of the provider.
        7. Adherence of the vendor to the Federal Decree-Law No. (45) of 2021 on the Protection of Personal Data and the ADEK terms and conditions, copyright policy, and data privacy policy with regard to the collection, use, and disclosure of information.
        8. Where relevant (e.g., learning application providers), educational quality, and age-appropriateness of content.
    - Schools must inform external providers that the provider is subject to Federal Decree-Law No. (45) of 2021 on the protection of personal data, as well as the ADEK terms and conditions, copyright policy and data privacy policy regarding the collection, use and disclosure of information.

Conclusion

This Policy reflect RSAD's commitment to creating a modern, digital and safe space for students development. The rules, standards and requirements included in this policy will improve work efficiency and protect the personal data of employees and students.