DUBAI GEM PRIVATE SCHOOL

STRIVE FOR EXCELLENCE

IT Security Policy

Introduction:

Dubai Gem Private School is committed to providing a safe and secure learning environment for students, staff, and visitors. This IT Security Policy outlines the guidelines and procedures we follow to protect the confidentiality, integrity, and availability of school-owned and managed information technology resources.

Scope:

- This policy applies to all users of Dubai Gem Private School's IT resources, including:
- Staff
- Students
- Parents and guardians
- Third-party vendors
- Visitors

Policy Objectives:

The primary objectives of this policy are to:

Protect sensitive data from unauthorized access, disclosure, alteration, or destruction.

Ensure the safe and reliable operation of all IT systems and infrastructure.

Comply with applicable data privacy regulations, including the UAE's Federal Law No. 13 of 2012 on the Protection of Personal Data.

Minimize the risk of cyberattacks and security incidents.

Endpoint Protection:

Dubai Gem Private School utilizes Sophos Endpoint Detection and Response (EDR) solution on all servers and computers to further enhance its security posture. This advanced solution provides proactive protection against known and unknown threats, malware, and ransomware attacks.

Acceptable Use:

All users of Dubai Gem Private School's IT resources must comply with the following acceptable use guidelines:

- **Data Protection:**

Use school-owned devices and accounts only for authorized purposes.

Do not share passwords or account information with others.

Download and install software only with prior approval from the IT department.

Report any suspected security incidents or data breaches immediately.

- **Network Security:**

Do not engage in activities that could harm the school's network, such as hacking or spreading malware.

Avoid accessing prohibited websites or content.

Use strong passwords and change them regularly.

- **Email and Online Communication:**

Do not send or receive inappropriate or offensive content via email or other online platforms.

Be mindful of privacy settings when using social media or other online services.

Password Policy:

All users must create strong passwords that are at least 8 characters long and include a mix of uppercase and lowercase letters, numbers, and symbols.

Consider implementing multi-factor authentication (MFA) for sensitive accounts.

Access Control:

Access to sensitive data will be granted on a need-to-know basis.

User accounts will have appropriate access levels based on their roles and responsibilities.

Regular reviews will be conducted to ensure that user access rights remain appropriate.

Incident Response:

Dubai Gem Private School has a documented incident response plan to address potential security incidents.

All users are required to report any suspected security incidents immediately to the IT department.

The IT department will investigate all reported incidents and take appropriate action to mitigate the impact and prevent future occurrences.

Software Security:

All school-owned devices must have antivirus and anti-malware software installed and kept up-to-date, even with Sophos EDR in place.

Windows OS updates and security patches must be applied promptly.

Implement a software inventory and approval process to control the apps and software used on school devices.

Review the security practices of cloud-based services (Google Classroom, Seesaw) and third-party services (Alpha ERP) to ensure they meet your standards.

Network Security:

Maintain separate networks for staff, students, and guests with appropriate firewall and VLAN configurations to isolate traffic and minimize risk.

Regularly monitor network activity for suspicious behavior and anomalies.

Implement wireless network security measures such as encryption and guest network restrictions.

Monitoring and Auditing:

Dubai Gem Private School reserves the right to monitor network activity and user accounts to ensure compliance with this policy.

All monitoring will be conducted in accordance with applicable data privacy regulations.

Policy Review and Updates:

This policy will be reviewed and updated on a regular basis to reflect changes in technology, threats, and regulations.

Reviewed: January 2024