مدرسة الشعاع الهندية
للبنات والبنين
Radiant Indian School
For Girls & Boys

RADIANT INDIAN SCHOOL FOR GIRLS AND BOYS,SHARJAH

IT INFRASTRUCTURE SECURITY POLICY

1. Introduction:

Radiant Indian School For Girls and Boys recognizes the importance of maintaining a secure IT infrastructure to protect sensitive data, ensure the reliability of systems, and mitigate the risk of cyber threats. This policy outlines the measures and guidelines for securing the school's IT infrastructure, including computer labs.

2. Scope

This policy applies to all IT assets, including hardware, software, networks, and data, owned or operated by Radiant Indian School For Girls and Boys, including the computer labs with 30 systems each.

3. Access Control

Access to computer labs and IT resources will be restricted to authorized individuals, including staff and students, through the use of unique usernames and passwords.

User accounts will be regularly audited to ensure compliance with access control policies, and inactive accounts will be disabled promptly.

Physical access to computer labs will be restricted to authorized personnel only, and security measures such as locks and surveillance cameras will be implemented to prevent unauthorized entry.

4. Software and Patch Management

Only licensed software approved by the school will be installed on computer lab systems, and unauthorized software will be promptly removed.

Regular software updates and security patches will be applied to ensure that systems are protected against known vulnerabilities and exploits.

Anti-virus software will be installed and updated on all systems to detect and prevent malware infections.

5. Network Security

Network traffic within the school's IT infrastructure will be monitored and filtered to prevent unauthorized access and malicious activities.

Firewalls and intrusion detection/prevention systems will be deployed to protect against external threats and unauthorized access attempts.

Wireless networks will be secured with strong encryption and authentication mechanisms to prevent unauthorized access.

6. Data Protection

Sensitive data stored on computer lab systems will be encrypted to protect against unauthorized access in case of theft or loss.

Regular data backups will be performed to ensure data integrity and availability in the event of data loss or corruption.

Data transmission over the school's network will be encrypted using secure protocols to prevent interception and eavesdropping.

7. Incident Response

Procedures will be established for responding to IT security incidents, including data breaches, malware infections, and unauthorized access attempts.

Incident response plans will outline roles and responsibilities, escalation procedures, and communication protocols for effectively managing security incidents.

Security incidents will be promptly investigated, documented, and reported to the appropriate authorities as required by law.

8. Training and Awareness

Staff and students will receive regular training on IT security best practices, including password hygiene, phishing awareness, and data protection.

Awareness programs and campaigns will be conducted to educate the school community about the importance of IT security and their role in maintaining a secure environment.

9. Policy Review

This policy will be reviewed annually to ensure its effectiveness and relevance in addressing emerging IT security threats and vulnerabilities.

Feedback from staff, students, and other stakeholders will be considered in the review process to identify areas for improvement.

10. Policy Approval

This policy has been approved by Ms. Alka Suxena, Principal of Radiant Indian School For Girls and Boys.