CROWN PRIVATE SCHOOL
مدرسة كراون الخاصة
British Curriculum المنهاج البريطاني

INCIDENT RESPONSE POLICY

PROCESS NAME:	Incident Response Policy	**CREATION DATE:**	10/09/2022
PROCESS MANAGER:	IT Administrator	**LAST REVISION:**	05/02/2025
PREPARED BY	Rajeesh Kumar – IT-Admin	**APPROVED BY**	Dr. Kishor Pillai- Principal
APPLIES TO:	All Staff All Parents All Children	**RELATED DOCUMENT(S):**	Disaster Recovery Policy

1. **Introduction**
   The purpose of this Incident Response Policy is to establish a framework for responding to cybersecurity and IT-related incidents at Crown Private School. The policy ensures timely detection, reporting, and mitigation of security incidents to minimize damage, protect sensitive information, and ensure business continuity.
2. **Scope**
   This policy applies to all employees, students, IT staff, contractors, and third-party vendors who access or manage IT systems, networks, or data at Crown Private School. It covers all security incidents, including data breaches, malware infections, unauthorized access, and service disruptions.
3. **Incident Response Team (IRT)**
   A designated Incident Response Team (IRT) will be responsible for handling cybersecurity incidents. The team comprises:

- IT Manager (Team Lead)
- Network Administrator
- System Administrator
- Data Analyst
- Legal Representative (if necessary)
- Communication Officer

4. **Incident Classification**
   Incidents are categorized based on severity and impact:

- **Low:** Minor issues with minimal impact, such as spam emails.
- **Medium:** Moderate disruptions, such as unauthorized access attempts.
- **High:** Critical incidents affecting operations, such as ransomware attacks or data breaches.

5. Incident Response Process

The response process follows these key phases:

5.1. Identification

- Detect and validate security incidents through monitoring tools, user reports, and automated alerts.
- Verify the authenticity and severity of the incident.

5.2. Containment

- Isolate affected systems to prevent further damage.
- Implement temporary measures to limit the spread of the incident.

5.3. Eradication

- Identify and eliminate the root cause of the incident.
- Remove malicious software, unauthorized access, or compromised credentials.

5.4. Recovery

- Restore affected systems and data from secure backups.
- Verify system integrity before reconnecting to the network.
- Monitor systems to prevent recurrence.

5.5. Reporting and Documentation

- Document all findings, actions taken, and lessons learned.
- Report serious incidents to regulatory authorities if required.
- Conduct a post-incident review to improve future responses.

6. Roles and Responsibilities

- **IT Staff:** Detect, report, and mitigate incidents.
- **Employees & Students:** Follow security best practices and report suspicious activities.
- **IRT:** Coordinate and lead incident response efforts.
- **Management:** Provide resources and ensure compliance with policies.

7. Communication and Notification

- Notify affected stakeholders, including staff, students, and parents, if necessary.
- Maintain clear and transparent communication while ensuring confidentiality.
- Coordinate with law enforcement and regulatory bodies if required.

8. Compliance and Legal Considerations

- Adhere to UAE Data Protection Laws and GDPR compliance requirements.
- Ensure all incident response actions align with school policies and legal obligations.

9. Training and Awareness

- Conduct regular training for staff and students on cybersecurity awareness.
- Perform simulated incident response exercises to enhance preparedness.

10. Review and Updates

- This policy will be reviewed annually or after significant incidents to incorporate improvements.
- Updates will be communicated to all relevant stakeholders.

This Incident Response Policy ensures Crown Private School is prepared to handle cybersecurity incidents effectively, minimizing disruptions and safeguarding sensitive data.

-