Group Policy

Cyber Incident Response

30 March 2025

Key Facts

- This policy establishes the approach and expectations for responding to and managing cyber security incidents across Cognita Group.
- Cognita Group must have an overarching cyber incident response plan which is maintained by the Group Cyber Security Team.
- Each region must have their own cyber incident response plan which aligns to the Group plan.
- Cyber incident response plans must detail members of a cyber security incident response team.
- The Group Cyber Security Team must have visibility of all cyber security incidents across the regions.

Document Control

Title	Group Policy – Cyber Security Incident Response
Author	James Tallon (JT), Peter Purwin (PP)
Owner	Reena Shah (RS)
Subject	Cyber Security Incident Response
Classification	Internal
Review Date	28 March 2026

Revision History

Revision Date	Reviser	Previous Version	Description of Changes
-	JT, PP	-	Creation of Group Cyber Security Incident Response Policy

Document Approvals

Name	Title	Date
Cyber Security Steering Group (CSSG)	Senior Governing Body for Cyber Security Across Cognita	28 February 2025
Group Executive Team	Group Executive Leadership Team	28 March 2025

Document Distribution

Role(s)	Method
Group IT	Email
Regional IT and leadership	Email
CSSG	Email, meeting
Group Executive Team	Email
Group and Regional Legal Team	Email
Group and Regional Communication Team	Email
Group and Regional Safeguarding Team	Email

Associated Documents

Title
Group Cyber Incident Response Plan
Regional Cyber Incident Response Plan

Contents

1. Definitions

Cognita Group (the "Group") refers to Cognita Holdings Limited and its subsidiaries, affiliated schools, and related entities globally. This includes all educational institutions, administrative offices, and operational units under the Group's ownership or control.

Cyber Security Incident is an event that threatens the confidentiality, integrity, or availability of an information system or its data.

Cyber Security Incident Response Team (CSIRT) is a designated group within Cognita tasked with managing cyber security incidents. Comprising both technical experts and management, the team is authorised to make critical decisions to minimise the impact of incidents and protect the Group.

Cyber Incident Response Plans (CIRP) are structured documents that outline the procedures and protocols Cognita Group must follow when responding to a cyber security incident. They include communication structure for both internal and external stakeholders and emphasise the importance of reviewing and updating the plan after incidents to improve future responses.

Digital Assets refers to all IT systems, software, data, and related resources that belong to or are part of the Groups digital ecosystem. This includes, but is not limited to, hardware, applications, databases, networks, and any other electronic or digital resources used by the Group.

Employees refers to all individuals affiliated with Cognita Group, including full-time and part-time staff, contractors, consultants, and any other personnel engaged for short-term or specific projects. This encompasses anyone who performs duties or provides services on behalf of the Group, regardless of their employment status or duration of engagement.

In-band communication refers to the use of standard day-to-day communication channels, such as email, messaging platforms (like Teams), and ticketing systems, for exchanging information and managing tasks during a cyber security incident response.

Out-of-band communication involves using alternative channels for communication that are separate from the standard tools, such as phone calls, text messages, or direct messaging apps, to ensure secure and reliable communication during a cyber incident response.

Restricted data is highly valuable and sensitive data that, if exposed, could cause significant harm to Cognita. This includes data that could negatively impact Cognita's competitive position, violate regulatory or contractual obligations, harm the company's reputation, or pose identity theft risks.

Target Response Time is an agreed timeframe for responding to an incident, determined by the severity of the incident. Response is defined as the time it takes a team member to actively begin addressing the identified incident, within the business hours where the incident takes place.

2. Policy Review Cycle

2.1 This policy will undergo a review on an annual basis or sooner if deemed necessary by the Group Cyber Security Team or Cyber Security Steering Group. A review may be triggered by significant cyber security incidents, regulatory changes, or the introduction of new technologies or processes. The review aims to ensure this policy remains effective in addressing evolving security threats, technological advancements, and changes in regulatory requirements. All updates to the policy must be shared with regional IT Teams, CSIRT's and relevant staff and be approved by the Cyber Security Steering Group (CSSG) and Group Executive Team.

3. Purpose

3.1 The purpose of this policy is to establish Cognita's approach for responding to and managing cyber security incidents, leveraging NIST CSF 2.0 and SP 800-61 to ensure alignment to industry good practices. It sets clear expectations and responsibilities for addressing incidents effectively, with the following objectives:

- To protect Cognita's digital assets and ensure their confidentiality, integrity, and availability.
- To minimise the impact of cyber security incidents on the Group's operations, reputation, and stakeholders.
- To maintain business continuity and swiftly restore normal operations following an incident.
- To comply with applicable regulations, industry standards, and contractual obligations related to cyber security.

By defining a structured framework for incident response, this policy supports Cognita's commitment to proactive risk management, robust security practices, and safeguarding the interests of its employees, students, and partners.

4. Scope

This Policy applies to all Cognita Group companies and schools worldwide ("Cognita" or "Group") and to all employees, whether permanent or temporary, including teachers, staff, administrators and third parties. It applies to all cyber security incidents relating to the organisation's assets including but not limited to organisational data, hardware, software, people, processes, IP, financial assets and reputation.

All exceptions to this policy must be requested using the Cyber Security Exception Request form. Exceptions will be evaluated on a case-by-case basis and be approved by the Group Cyber Security Team, with final sign off from the Cyber Security Steering Group (CSSG).

5. Policy Statements

5.1 Cyber Incident Response Plans

5.1.1 Cognita Group must have an overarching Group Cyber Incident Response Plan (CIRP) which is managed and maintained by the Group Cyber Security Team. This plan will serve as the framework for cyber incident response across Cognita Group.

5.1.2 The Group CIRP must be signed off by both the Group Executive Team and Group Head of Cyber Security.

5.1.3 Each region must have a documented regional CIRP which aligns to the Group CIRP, following Group approved formatting standards to ensure consistency.

5.1.4 Regional CIRP's must be tailored to address local regulatory requirements, operational context and risks for the region and/or countries it covers.

5.1.5 Regional CIRP's must be signed off by the Regional CEO and Group Head of Cyber Security.

5.1.6 CIRP's must include a list of cyber incident categories, allowing prioritisation of incidents based on severity.

5.1.7 CIRP's must have a designated Cyber Security Incident Response Team (CSIRT) responsible for managing P1 (Critical) and P2 (High) cyber security incidents.

5.1.8 All CIRP's must include a primary and secondary in-band communication method (e.g. email, tickets, teams).

5.1.9 All CIRP's must define a common alternative out-of-band communication method.

5.1.10 Members of the CSIRT must have their contact details documented and circulated as part of their respective CIRP's, and these details must be updated at least annually.

5.1.11 CIRP's must define testing requirements and at a minimum undergo yearly testing with a simulated test conducted at least every two years. The aim of these tests is to identify and remediate gaps, along with ensuring effectiveness.

5.1.12 The Group Cyber Security Team must identify metrics for monitoring both the compliance with and effectiveness of this policy.

5.1.13 The Group Cyber Security Team must have visibility of all cyber security incidents that occur across the Group.

5.2 Cyber Security Incident Response Teams

5.2.1 Cyber Security Incident Response Teams (CSIRT) must have the following roles documented within their CIRP's.

- **Group Cyber Security Incident Response Manager:** The Group Cyber Security Team member responsible for managing and coordinating response to incidents that require the formation of the CSIRT. This includes ensuring the incident is managed throughout its lifecycle, escalating to Management, and maintaining clear communication with relevant stakeholders.
- **Regional Cyber Security Manager:** A dedicated cyber security resource with in-depth knowledge of their specific region. They support the Group

Cyber Incident Response Manager and help coordinate stakeholders within their region to ensure effective incident response.

- **Regional IT Director:** The IT director who has oversight of the IT landscape within their region. They ensure that additional technology personnel can be called upon to assist as needed and own the escalation process within their specific region.
- **Subject Matter Experts (SME's):** Person/s across the business who support cyber incident response activities. They possess key business or technical knowledge, enabling effective incident response.

5.2.2 Depending on the nature of an incident, additional roles or functions from across the business may be required to assist**.** This is further detailed in 5.4

5.2.3 CSIRT members, or those that may be routinely involved in cyber incident response must receive training at least yearly, ensuring they understand their role and responsibilities to fulfil the required function. The Group Cyber Security Team, with support from Regional IT Directors are responsible for coordinating training, ensure CSIRT members are appropriately trained to fulfil their duties.

5.3 Cyber Incident Severities

5.3.1 All CIRP's must adhere to the severity levels and target response time noted in the below table (table 1).

5.3.2 For Medium (P3) and Low (P4) cyber security incidents, a Cyber Incident Responder shall be appointed to manage the incident through its lifecycle. This individual is responsible for triaging, responding to, and escalating incidents as needed. Examples of roles that could fulfil this responsibility include service desk analysts, school technicians, or dedicated cyber security analysts.

Severity	Target Response Time	Definition	Management Responsibility
Critical (P1)	1 hour	A critical incident that demands immediate attention. It significantly disrupts Cognita, has the potential to cause a substantial financial loss, or poses a considerable impact on overall business continuity.	CSIRT
High (P2)	4 hours	A major incident with significant impact, potentially involving the exposure of restricted data requiring notification to regulators or other relevant parties. While operations may continue, systems or services in one or more regions could be affected, leading to disruption.	CSIRT
Medium (P3)	1 day	A moderate incident that has a noticeable but manageable impact. It may cause inconvenience or affect systems without disrupting overall operations.	Cyber Incident Responder

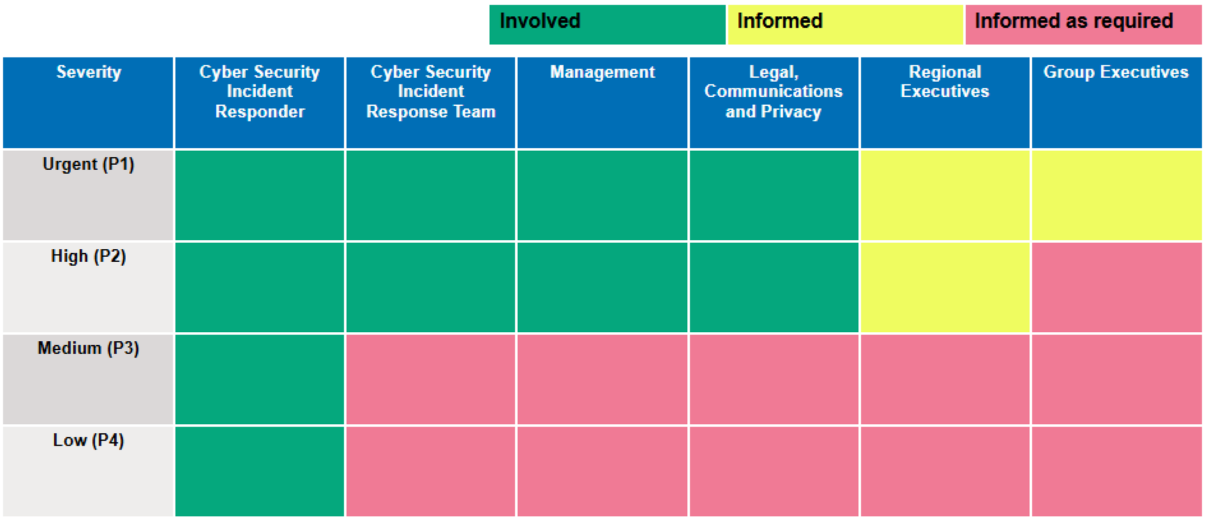
Low (P4)	3 days	A minor incident with minimal impact. It involves isolated issues that do not disrupt operations and pose little to no risk to organisational performance.	Cyber Incident Responder

Table 1 – Incident Severity and Target Response Time.

5.4 Incident Response and Escalation

5.4.1 At times, additional roles or functions across the business may need to be engaged or informed of a cyber security incident. The escalation and communication matrix outlined below (figure 1) must be used to identified who needs to be engaged or informed based on the severity of the incident. Functions that may be required to support cyber incident response include.

- **Cyber Incident Responder:** The individual/s responsible for initially managing cyber security incidents. This role involves initial triaging, responding to an escalating cyber security incidents as needed. Examples of roles that could fulfil this responsibility includes service desk analyst, school technicians or dedicated cyber security analyst.
- **CSIRT:** A dedicated team formed of key personnel to manage P1 (Critical) and P2 (High) cyber security incidents. This team forms the core group in a significant cyber related incident, engaging additional stakeholders as required.
- **Management:** This function involves individuals who need to be informed when P1 (Critical) or P2 (High) cyber incident occurs. They are responsible for evaluating the business impact and further escalating the matter if necessary. Examples of roles that could fulfil this responsibility include school leadership, directors, technology leads and head of functions.
- **Legal, Communications and Privacy:** Teams or individuals that possess specific knowledge in these areas. They assist by providing analysis and recommendations based on their expertise to the CISRT and Management. They may also be called upon to conduct tasks in accordance with timelines set during incident response activities.
- **Regional Executive:** A person with the authority to make key decisions that affect their specific region during an incident.
- **Group Executive:** A person with the authority to make key decisions that may impact multiple regions or the organisation.



🟩 Involved	🟨 Informed	🟥 Informed as required

Severity	Cyber Security Incident Responder	Cyber Security Incident Response Team	Management	Legal, Communications and Privacy	Regional Executives	Group Executives
Urgent (P1)	🟩	🟩	🟩	🟩	🟨	🟨
High (P2)	🟩	🟩	🟩	🟩	🟨	🟥
Medium (P3)	🟩	🟥	🟥	🟥	🟥	🟥
Low (P4)	🟩	🟥	🟥	🟥	🟥	🟥

Figure 1 – Escalation and Communication matrix

5.4.2 Any safeguarding concerns identified during cyber incident response must be reported to respective Safeguarding Teams.

5.4.3 The Group Cyber Security Team must identify and retain an external incident response partner. The CSIRT is responsible for assessing whether escalation to an external partner is necessary. Escalation must only occur after approval has been provided by the Group Head of Cyber Security or a Senior Leader withing Group IT.

5.4.4 All P1 (Critical) and P2 (High) incidents must have a cyber incident report generated as part of the incident response which follows requirements defined in the Group Incident Response Plan.

5.4.5 All timelines and recorded timeframes must be noted in Coordinated Universal Time (UTC).

5.4.6 Any risk resulting from a cyber incident must be documented in the regions risk register.

6. Roles & Responsibilities

6.1 Cyber Incident Responder

6.1.1 Act as the first line of defence in responding to cyber incidents within the Group or regions.

6.1.2 Conduct initial triaging and response for cyber security incidents.

6.1.3 Escalate cyber security incidents promptly, ensuring information is accurately captured and required stakeholders are engaged.

6.1.4 Document all information and steps taken in the defined tool or system used for cyber incident response activities.

6.2 Cyber Security Incident Response Team (CSIRT)

6.2.1 Manage P1 (Critical) and P2 (High) cyber security incidents, or those requiring further resource or attention.

6.2.2 Coordinate and oversee incident response activities across regions, countries and schools, ensuring a unified and efficient approach.

6.2.3 Group Cyber Incident Response Manager

- Lead the CSIRT and ensure required stakeholders are engaged.
- Ensure thorough documentation of all incidents, including the nature of the incident, actions taken, and outcomes, to support post-incident analysis and reporting.
- Analyse and evaluate the effectiveness of responses to cyber incidents, documenting lessons learned and providing reports to senior management for review.

6.2.4 Regional Cyber Security Manager

- Support the Group Cyber Incident Response Manager and act as a secondary incident manager.
- Coordinate resources within the region and assist regional management in understanding required actions.

6.2.5 Regional IT Director

- Ensure support staff are available to assist as required during cyber security incident response.
- Provide key input and decision making for aspects that affect the regional, escalating to management as required.

6.2.6 Subject Matter Experts

- Provide key business and technical support during cyber incident response activities.
- Be available to support cyber incident response efforts, ensuring direction and timings are met throughout cyber incident response activities.

6.3 Management

6.3.1 Be available to support cyber incident response efforts, ensuring resources are available as required to support.

6.3.2 Evaluate business impact and further escalate incidents if necessary.

6.4 Legal, Communications and Privacy

6.4.1 Provide subject matter expertise to ensure that cyber incident response meet’s applicable laws, regulations and reporting requirements.

6.4.2 Be available to conduct tasks as part of cyber incident response, meeting defined timelines set by the CSIRT and supported by management.

6.5 Regional Executives

6.5.1 Review and support regional CIRP’s, ensuring resources are allocated and authorised to conduct appropriate incident response activities.

6.5.2 Provide decision and approval for incident response efforts that affect their region.

6.6 Group Executives

6.6.1 Review and support the Group CIRP, ensuring resources are allocated and authorised to conduct appropriate incident response activities.
6.6.2 Provide decision and approval for incident response efforts that affect the Group.

6.7 Cyber Security Steering Group (CSSG)

6.7.1 Provide strategic oversight and commitment to the implementation and enforcement of the Group Cyber Incident Response Policy.
6.7.2 Review and approve policy updates and revisions based on recommendations from the Group Cyber Security Team.
6.7.3 Ensure alignment of the incident response policy with the Group's overall risk management strategy.

6.8 Group Cyber Security Team

6.8.1 Develop, implement, and maintain the Group cyber incident response policy in accordance with industry standards and good practice.
6.8.2 Conduct regular reviews and testing of this policy and related plans to assess the effectiveness, identifying improvement opportunities.
6.8.3 Provide training and support for employees, CSIRT’s and IT Teams to enhance cyber security response effectiveness.
6.8.4 Report P1, P2 and notable cyber security incidents during Cyber Security Steering Groups.

6.9 Employees

6.9.1 Promptly report suspected cyber incidents or suspicious activities to local IT or management using designated channels.
6.9.2 Cooperate with local IT and Group Cyber Security Team during investigations, providing any relevant information or assistance as needed.
6.9.3 Avoid interfering with ongoing investigations or attempting self-resolution of incidents.
6.9.4 Participate in awareness programs and adhere to cyber security policies to minimise risks.

6.10 External Resources

6.10.1 Support incident response efforts as defined in contractual obligations, ensuring timely assistance and resource availability.
6.10.2 Cooperate with the Group Cyber Security Team and regional IT teams to address vulnerabilities or breaches affecting systems.