2.1 Contingency and Adverse Effects Policy

Policy No.	2.1
Version Date	14th April, 2026
Approved by	SMT
Policy Group	Operations
Version number	V01
Next review due	April 2027
External Reference points	National Centre for Cyber Security https://nccs.pk/ Academic Regulations of Partner universities/organisations

Version Control Previous Version	New Version	Date	Update/Notes
-	V01	14-04-2026	New policy issued.

Introduction

This Contingency and Adverse Effects Policy involves identifying and preventing adverse events and ensuring that lessons are learned so they may be prevented from occurring in future. Adverse events can pose risks to IVY Academic Network operations and this policy provides a means for ensuring that the type of adverse effects that may affect are understood and there are plans in place for dealing with them and mitigating them.

This policy uses the following abbreviations: SMT (Senior Management Team), CIMT (Critical Incident Management Team), CIRT (Cyber Incident Response Team), HOI (Head of Institute), HO (Head of Operations), and MD (Managing Director).

This policy is reviewed annually by the Senior Management Team, or sooner where a significant incident, regulatory change, or identified weakness in existing arrangements makes an earlier review necessary.

This policy should be read alongside related institutional policies where relevant, including the Child Safeguarding and Prevent Policy (for incidents involving harm to children or vulnerable adults), the Data Protection Policy (for incidents involving personal data), and the Complaints Policy (for challenging how an incident was handled).

Purpose and Scope

This policy prepares IVY Academic Network for the effects of something happening that will potentially have a detrimental impact on the achievement of organisational objectives, or even in some cases on the existence of IVY Academic Network. It includes risk management, which is the process of preparing for and mitigating the likelihood and potential consequences of a detrimental event occurring. Health and Safety risks are assessed and managed by IVY Academic Network Health and Safety Policy. All other risks are assessed and managed by the Student Protection Plan July 2024 and a Risk Register.

IVY Academic Network aims to be prepared to deal with the impact of incidents that may harm IVY Academic Network, its students, staff and other stakeholders. To this end it will

- Identify a range of adverse events that can impact negatively on IVY Academic Network, its students and other stakeholders.
- Identify a range of critical incidents that may occur
- Ensure the development and ongoing review of risk for the IVY Academic Network and all its activities
- Determine the method of assessing and managing risks
- Ensure staff understand their responsibilities in terms of risk ownership
- Provide an updated Contingency and Adverse Effects Plan that is fit for purpose, and aligned with the Student Protection Plan

Identifying Adverse Events

An adverse event may impact on IVY Academic Network in the following ways:

- IVY Academic Network is unable to meet its deadlines for the publication of results and handing out of certification with may impact in individual student plans and progress
- IVY Academic Network fails to adequately identify academic misconduct and malpractice which impacts on the credibility of IVY Academic Network and the award
- Rising costs to students due to an unforeseen event e.g. moving to a new location that may prevent them from being able to complete their course
- IVY Academic Network is prevented from delivering an academic programme leading to an award
- An assessment does not ensure the standards of the qualification are secure
- An assessment does not allow for a consistent distinction between the assessment of student work at different levels
- The reputation of IVY Academic Network if is subjected to a criminal investigation or faces sanction from regulators or awarding organisations
- The reputation of IVY Academic Network if a member of the Senior Management Team is subjected to a criminal investigation or other disciplinary proceedings
- Poor, inaccurate or misleading public information that impacts on student expectations and achievements

Procedure for dealing with an Adverse Event

Reporting an event or near miss

Staff must report the following to the Head of Operations if an adverse event occurs and escalate it to the Managing Director if necessary.

Your Name

Your Contact

What adverse event has occurred?
Describe it briefly

Who are directly affected by the event?

Date and time of the event

Location of the event

What caused it to happen?

What action has been taken so far?

How severe is the event?
Low ☐
Medium ☐
High ☐

Adverse Events Team

If there is an adverse event of the kind identified in the section above, the Adverse Events Team will investigate it and make recommendations to the Senior Management Team if required:

Head of Institute
Head of Academics
Head of Compliance

Head of Quality

Records of adverse events and critical incidents, including reports, investigation findings and correspondence, are retained securely for a minimum of six years from the date the matter is closed, or for as long as required by an active case or applicable legal requirement.

Notification to Awarding Organisations

It may be necessary to report some critical incidents or adverse effects to IVY Academic Network's Awarding Organisations if the incident or adverse effects lead to one of the following:

IVY Academic Network becomes insolvent or faces bankruptcy proceedings.
There is any change in ownership of IVY Academic Network.
There is a significant change to the way in which the IVY Academic Network is governed or its legal status.
IVY Academic Network should merge with any other entity.
There has been event that adversely affects student studying for the programmes offered in collaboration with Partner Universities.
A student wishes to transfer to another centre offering the same award

The IVY Academic Network Adverse Effects Team provided above will determine if there is a need to inform the awarding organisation and if there is, will appoint one person to contact the awarding organisation without delay and provide the following:

How many students are affected
How serious the event is
If the event is due to misleading information published by IVY Academic Network
The qualifications and units affected if relevant
How the incident was first reported
All the parties involved and aware of the incident
A plan of action showing what steps have already been taken and what is next

Identifying Risks

The risk management process, excluding risks that fall more generally under the category of Health & Safety threats and hazards, are based on an assessment of risks including those identified in the Student Protection Plan and Risk Register. Risks may be added or removed, and the Risk Register is updated every four months. The following list, which is not exhaustive, includes risks that may be identified and assessed in the Risk Register:

Student Recruitment
Admissions Process
Student Engagement Progression
Student Learning
Resources to Enhance the Student Experience
Key Staff Retention
Financial Resources
Information Resources

External Policy Environment
Student Voice
Student Experience
Marketing Strategy
Governance
Reputation
IT Infrastructure and Data Protection
Growth Targets
Closure of the IVY Academic Network
Closure of a Course or Courses
Change in Course Content
Change in Location
Limitations due to the Pandemic or Natural Disaster
Change in law

Identifying Critical Incidents

The following are examples of critical incidents that may occur. This list is not exhaustive:

The loss of data or breach of confidentiality through cyber attack
A student, staff member or other stakeholder dies as the result of an accident, illness or crime
A student, staff member or other stakeholder has a serious injury
A student, staff member or other stakeholder is physically attacked and harmed
Collapse of IVY Academic Network buildings.
Threats to public health, such as outbreaks of meningitis or a pandemic.
Severe weather conditions disrupting normal activities.
Accidents involving transportation.
Civil disturbances or acts of terrorism.

Assessing Risk – Student Protection Plan

The risks in the table below include a likelihood and an impact score of 1-5. A low score of 1 or 2 means a very low risk, and a high score of 4 or 5 is a very high risk. When the likelihood and impact score are multiplied together, the overall rate of risk can be identified as follows:

1-5
Very Low Risk
6-10
Low Risk
11-15
Medium Risk
16 – 20

High Risk
21 – 25
Very High Risk

All risks are explained according to how well they are currently being managed of controlled. Deadlines are also provided for further mitigations that are planned to help prevent the risk from occurring and to minimise its impact if it does.

Senior Management Team

The Student Protection Plan and the overall management of risk including the review, update and implementation of this policy is the responsibility of the Senior Management Team (SMT) which carries out the following functions at its quarterly meetings:

- Overseeing the effectiveness of and adherence to established policies in relations to risk and risk management including this policy
- Revising and enhancing relevant policies and procedures to address existing risks effectively.
- Assessing the IVY Academic Network's risk management framework to guarantee all essential risk areas are addressed.
- Identifying and suggesting new risk areas as they become necessary.
- Implementing measures to mitigate risks and reduce their potential adverse impacts.

Risk Owners

Each risk identified must have a risk owner, who is responsible for ensuring their assigned risk area is effectively monitored and mitigated. The risk register remains live and is updated by all risk owners every quarter or soon if the urgent need arises.

General Staff Responsibilities

All IVY Academic Network staff members are tasked with identifying, reporting, and managing risks effectively. Specific risk ownership is delegated to staff members by the Senior Management Team. Staff are required to provide updates on risk controls and risk mitigation plans for the risks assigned to them, including the execution of strategies to reduce risks, ensuring these align with broader planning procedures and activities.

Head of Operations (HO)

The IVY Academic Network Head of Operations is responsible for ensuring effective risk management processes and competent managers are consistently in place. Comprehensive risk assessment and management must be conducted to identify and mitigate risks across all IVY Academic Network services, whether delivered online or on-site at any campus. Risk assessments should be integrated into the planning, development, and expansion of IVY Academic Network

provisions, facilities, and resources.

Risk Management Process

The process of risk management at IVY Academic Network has the following steps:

The control status and implementation of all risk mitigation plans is monitored by risk owners
Risk owners update the control status and mitigation plans of all risks they are responsible for
Risk owners report on the risks they are responsible for to the Senior Management Team (SMT) every quarter.
The Senior Management Team discusses and approves the updated risk register together with all control updates and mitigation plans every quarter

Critical Incident

Aim

Whenever a critical incident occurs, there must be a critical incident management team in place ready and able to react promptly and effectively so that the any harm or damage is either prevented or minimised. An appropriate response from the (CIMT) must be in place quickly to informs all stakeholders and people at risk about the nature and extent of the incident and what steps are being taken to prevent or minimise harm or damage from occurring.

Critical Incident Management Team (CIMT)

Managing Director
Head of Institute
Head of Academics
Head of Operations
Head of Quality

Other staff or stakeholders may be co-opted as members of the CIMT if needed. CIMT may also contact partners who may support and participate in any emergency planning and mitigations. The MD will lead CIMT in taking steps to deal with any critical incident. In the absence of the MD, the HOI will lead the CIMT. The following scenarios provide some guidance on how critical incidents will be handled by CIMT.

Terrorist Incident Occurs

IVY Academic Network informs all its students, staff and other stakeholders to follow the government's recommendations on dealing with a terrorist incident, especially if it involves someone with a weapon such as a gun or knife or any explosives. The key government recommendation involves moving away from danger, staying out of sight, and alerting the authorities as soon as it is safe to do so if a terrorist incident occurs anywhere including on excursions outside or in an IVY Academic Network building or other facility occupied by IVY Academic Network students, staff and stakeholders engaged in activities organised by or on behalf of IVY Academic Network.

If a critical incident such as a terrorist attack affects IVY Academic Network stakeholders during activities arranged by or for IVY Academic Network stakeholders, the following steps must be taken:

The relevant emergency services (e.g., Police 15, Rescue 1122) must be contacted.
The Head of Operations must be informed.

The Head of Operations will organise the required action which will include:

Arranging transportation if necessary to take people home or to safety
Informing the Critical Incident Management Team (CIMT) members
Calling a meeting of the CIMT to agree on a plan if necessary

The CIMT briefs and advises students and staff about the incident and what they need to do to stay safe.

Following any critical incident, affected students and staff will be offered appropriate wellbeing support and, where required, referred for further support in line with the Student Support Policy.

Procedure for Handling Cyber Attacks

IVY Academic Network follows the guidelines set out by the National Centre for Cyber Security (see link below) in order to deal effectively with the detection, response and resolution of cyber incidents particularly to the extent that they may affect students.

https://nccs.pk/

Preparation and Prevention

IVY Academic Network takes the following steps to prepare for and prevent the likelihood and impact of cyber-attacks:

Maintaining an up-to-date inventory of IT systems, networks, and software to ensure that all impacts of cyber-attacks can be identified and rectified by IT staff
Conducting training in cybersecurity for staff and to a lesser extent for students
Implementing robust firewall and antivirus solutions across all devices in all campuses
Regularly backing up critical data to secure, off-site or virtual locations.
Carrying out periodic vulnerability assessments and penetration testing.

Detection and Reporting

IVY Academic Network proactively monitors all its IT systems for unusual activity using automated tools and manual checks. IVY Academic Network also instructs all staff and students on the need to notify the IVY Academic Network Cyber Incident Response Team (CIRT) as described below about any suspicious activity that may involve cyber threats and attacks, and these are investigated by CIRT. Low level incidents may be handled by the IT Manager alone. However, higher level incidents that may compromise service delivery or confidential data must be escalated to the CIRT.

Critical Incident Response Team

The Cyber Incident Response Team (CIRT) includes the following IVY Academic Network members:

Head of IT and Networking
Finance Manager
Managing Director
Head of Academics
Head of Operations
Head of Compliance

Critical Incident Response

The CIRT is activated as soon as there is a threat or actual cyber-attack that has be escalated by the IT Manager or other IT staff and the following steps are taken:

The incident is triaged in order to understand how the specific details of the incident including its type and severity
The cyber breach is contained by isolating affected systems or networks.
The incident is communicated to key stakeholders, including management, staff, and students.
Relevant authorities or regulators are notified (e.g., the relevant data protection authority) if personal data is involved.

Cyber-Attack Severity

The severity of a cyber-attack is determined according to the following three criteria:

Availability of data or systems following the attack and how this affects IVY Academic Network services to students and the support it provides to staff
Confidentiality of sensitive data and whether it has been stolen or leaked
Integrity of any data or systems that may have tampered with so they can no longer be relied upon

Severity Level
Description
Examples
Impact
Critical
Cyber-attacks causing severe disruption to essential operations, major data breaches, or compromising sensitive information.
Attack on student/staff personal data (e.g., identity theft). Breach of exam or assessment results or academic records. Complete system failure affecting teaching and learning platforms.
Students unable to take their exams or assessments or get their result in timely fashion. Most staff unable to work effectively. No access to systems, platforms or email accounts for course delivery. Legal and regulatory consequences. Loss of stakeholder trust. Loss of partnerships. Major reputational damage. Significant financial impact.
High (Less Critical)
Attacks disrupting operations but manageable with immediate action, targeting fewer sensitive systems or data.
Ransomware affecting administrative systems-Denial-of-service attack (partial, recoverable). Malware in library access platforms.
Up to 50% of students and staff are affected through loss of data and lack of access to systems or email accounts. Some examinations or assessments may be compromised. Temporary disruption to operations. Potential reputational harm. Costly
recovery measures
Medium

Minor cyber incidents with minimal disruption, affecting non-essential services or isolated issues. Phishing attempt targeting a few staff or students. Malware infecting individual devices. Low-scale unauthorised access.
Limited operational impact. Minimal reputational concern Quick resolution possible with minimal resources.

Mitigations if a Critical-Level Cyber-Attack Occurs

When dealing with a critical-level cyber-attack, IVY Academic Network will seek consultation with National Cyber Crime Investigation Agency https://www.nccia.gov.pk/ for the provision of IVY Academic Network's firewall.

- Immediately activate the Critical Incident Response Team (CIRT).
- Isolate affected systems to prevent further damage.
- Neutralize the threat by addressing vulnerabilities and removing malware or compromised accounts.
- Restore systems and data from backups, ensuring integrity checks are completed.
- Notify regulatory bodies and all stakeholders promptly.
- Engage cybersecurity experts for containment and resolution.
- Enhance security post-incident with updated protocols and employee training.
- Keep detailed records of all recovery actions taken.
- Support affected individuals, including offering guidance on protecting their accounts and data.
- See below for further guidance on mitigation measures for cyber-attacks affecting exams and assessments

Mitigations if a High-Level Cyber-Attack Occurs

- Escalate the issue to the Head of IT and Networking for immediate action.
- Isolate and restore affected systems from backups.
- Communicate with staff and students to manage disruptions.
- Identify vulnerabilities and address them with updated software patches.
- Keep detailed records of all recovery actions taken.
- Support affected individuals, including offering guidance on protecting their accounts and data.
- See below for further guidance on mitigation measures for cyber-attacks affecting exams and assessments

Mitigations if a Medium-Level Cyber-Attack Occurs

- Resolve the issue at the Programme Leadership level.
- Provide affected staff or students with support and guidance.
- Monitor for any signs of escalation.
- Review and adjust user access controls if necessary.

Cyber Attacks during Exams and Assessments

Dealing with a cyber-attack during exams and assessments requires a clear, focused approach to ensure minimal disruption and preserve the integrity of the examination or assessment process. In the event of an attack, the first priority must be the immediate containment of the incident to secure all digital systems related to exams and assessments. Communication with students and staff is vital; they should be informed promptly of any disruptions and provided with instructions on how to proceed. Alternative arrangements may need to be implemented, such as shifting to offline or manual examination methods if systems cannot be restored quickly. Additionally, a review of affected systems should be conducted to assess whether any exam or assessment data has been compromised, and necessary steps must be taken to recover or safeguard this information. IVY Academic Network must coordinate with relevant bodies, such as examining boards or regulatory authorities, to ensure compliance and transparency throughout the process. Once the situation has been resolved, steps should be taken to enhance security measures to prevent future occurrences during critical periods like exams.

Post-Incident Review

After a cyber-attack IVY Academic Network will conduct a thorough review that includes the following:

- Conduct a thorough analysis of the attack, identifying weaknesses and lessons learned.
- Update security measures and protocols based on findings.
- Provide a report to the Senior Management Team (SMT) on the incident and improvements made.
- Schedule follow-up assessments to ensure ongoing protection.
- Retain records of the incident, response actions and lessons learned for a minimum of six years, or for as long as required by an active case or applicable legal requirement.

Communication in a General Emergency Situation

A designated member of the Critical Incident Management Team (CIMT) will handle communication with emergency services using a mobile phone.

- A designated member of CIMT will communicate with media outlets on behalf of IVY Academic Network if required.

IVY Academic Network's primary contact line, **111-489-111**, will serve as the point of contact for incoming calls.

- IVY Academic Network may use an emergency 24-hour phone number if needed.
- Mobile phones will be used for all outgoing calls during the incident.

Staff managing incoming calls must maintain records of the date, time, caller details, and the content of the conversation.

- All calls will be recorded if possible.

A person nominated by the Critical Incident Management Team will handle all media enquiries and no-one else will communicate to the media including responding to emails or phones calls without approval by the Critical Incident Management Team.

Where to go in an Emergency

In an emergency, CIMT and any other stakeholder needing help, support or information should go to the **Control Centre** at IVY Academic Network's Head Office: Bahria Greens, Sector 1, Rawalpindi. If IVY Academic Network's Head Office is unsafe for any reason, IVY Academic Network CIMT will inform all stakeholders of an alternative location for the Control Centre during and immediately after a critical incident.