Enterprise Incident Management Plan

Change History

Date	Version	Created by	Description of change
2019-03	.1	[redacted]	Initial Draft for Zayo
2019-03	1.0		Approved, Final Publication, Distribution
2019-10	1.1		Updates to: IMT members and branding
2020-04	1.2		Updates to: IMT members, IMAT members, branding, and streamlining processes
2021-01	1.3		Updates to: IMT & IMAT Members
2024-06	1.4		Updates to document template
2024-09	1.5		Update to process workflow
2024-10	1.6		Updates per Operational and Systems Continuity Standard
2024-12	1.7		Review and suggested updates
2025-02	2.0		Finalize and Publish
2025-04	2.1		Update to add acquisition or sale section
2025-04	2.2		Review and suggested updates
2025-04	3.0		Finalize and Publish

Table of contents

1. Purpose, scope, and Users

Zayo Group and its subsidiaries and Zayo Europe and its subsidiaries ("The Organization") is committed to meeting and maintaining appropriate security policies, standards, and procedures in alignment with its business strategy and mission.

The Incident Management Plan (IMP) establishes a structure for efficient communication and coordination between Zayo teams, leadership and Crisis Management and Incident Management teams during a significant business disruption. Additionally, this document provides procedures to be used by the Zayo Incident Management Team before, during and after business disruptions in order to assist local teams performing incident response actions.

The specific objectives of the IMP are to provide guidelines to:

- Effectively managing information flows to and from the Zayo Leadership Team (LT) and the Zayo Incident Management Team (IMT), and other Zayo wide response teams during business disruptions as considered appropriate by the Zayo IMT Chair
- Coordinating recovery efforts across multiple locations
- Mobilizing a core group of Zayo leaders to assist the onsite Service or Process Recovery Teams with necessary resources and guidance
- Employee life and safety response and evacuation procedures through the Zayo Emergency Response Team (ERT) program

The IMP does not provide:

- Specific recovery procedures for recovery of critical business processes
- Disaster recovery procedures focusing on recovery of IT applications and infrastructure
- Executive procedures for Corporate crisis communications and management

Users of this Plan are employees, contractors, and interns of the Organization, and will be referred to as "User" throughout all Security documentation.

Vendors and partners will be referred to as "Supplier" throughout all Security documentation. Suppliers are subject to compliance with the portions of this Plan relative to their services as agreed upon contractually.

2. Exceptions

In certain circumstances, exceptions to this Plan may be allowed based on demonstrated business need, or to apply local relevant laws and regulations. Exceptions to this Policy must be formally documented and approved by the Security team and will be treated as issues as part of the Risk Management program. Issues created from policy exceptions must have a remediation plan and may result in a risk for assessment, remediation, or acceptance by a control owner.

3. Plan maintenance and testing

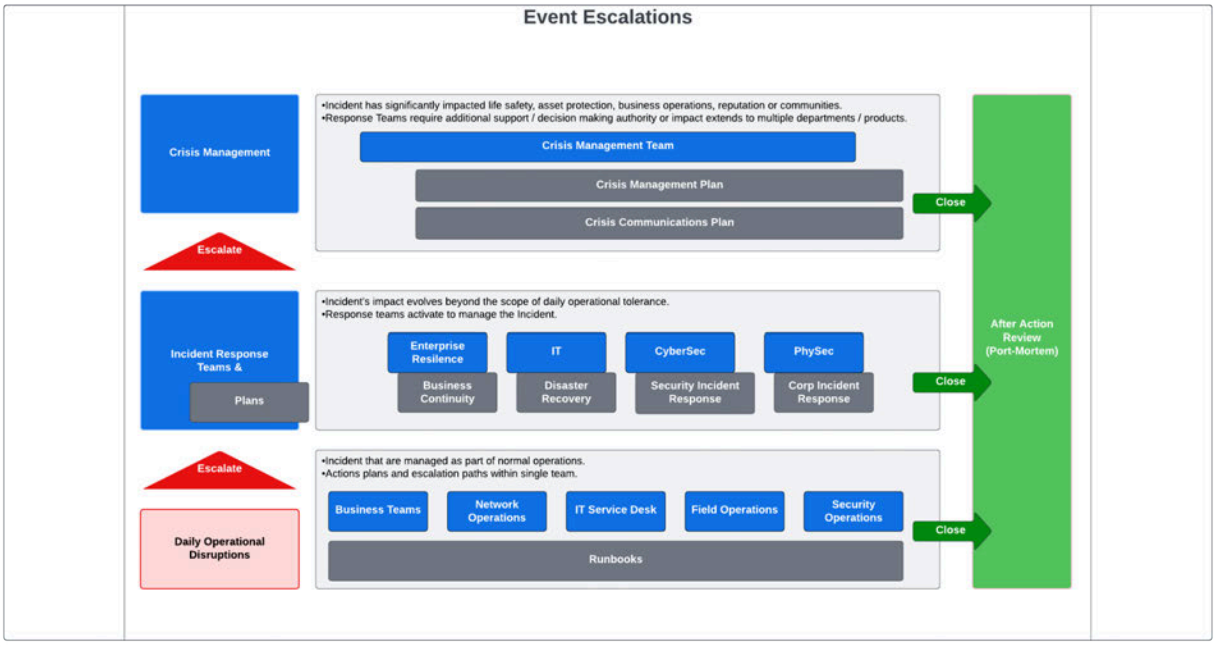
Plan maintenance and testing is the responsibility of each plan owner, with assistance from the enterprise resilience program. Plan owners maintenance responsibilities include:

- Perform annual review and testing of plans, unless otherwise determined
- Update the plans at least annually unless otherwise determined or as required based on test results
- Keep the Crisis Communication Plan updated

4. Other response plans

Zayo's collection of plans, procedures and information were developed for an integrated solution that ensures the continuation of your service in the event of a critical service interruption due to a serious natural, manmade, local or regional disaster. The plans include procedures that relate to vital areas of Zayo's business: Voice, Data, Information Technology (IT) and Operational Support Systems (OSS).

The Zayo network is continuously monitored throughout our service region and immediately activates the appropriate recovery teams, who then invoke their plans, if a disruption occurs. The Crisis Management and Communications Plans define escalation procedures and how integrated response occurs.

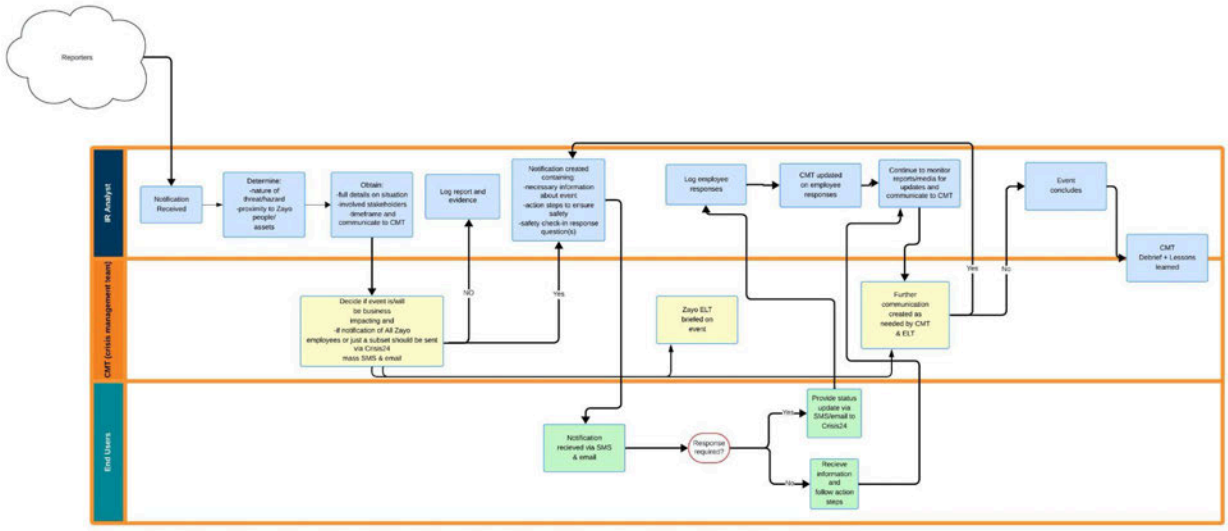


Our Event Escalation Model operates on a tiered approach, with first responders (Tier 1) at the forefront. These dedicated individuals are equipped to address and mitigate incidents in real-time, ensuring immediate action to minimize any potential disruption. Their vigilance and expertise lay the foundation for our operational resilience.

In the event that an incident transcends the capacity of Tier 1 responders, our model seamlessly escalates to Tier 2 – specialized response teams equipped with advanced skills and resources. These teams act as the second line of defense, providing support and expertise to handle complex challenges and ensure a comprehensive approach to incident resolution.

Furthermore, recognizing the evolving nature of incidents, our model incorporates a crisis escalation mechanism. When a situation demands heightened attention and intervention, Tier 2 response teams can escalate seamlessly to crisis management. This ensures that Zayo is prepared to handle even the most critical scenarios, deploying resources and strategies commensurate with the severity of the incident.

5. Incident response workflow



6. Incident assessment levels

INCIDENT ACTIVATION TRIGGERS	HUMAN	NATURAL	INFRASTRUCTURE	TECHNOLOGICAL
Example	Pandemic, workforce outage, terrorism, civil disorder, Corporate/Industry Incident	Severe weather - tornado, snow storm, flood, etc. (hurricanes are typically not IMT events)	Power outage, building fire / explosion, hazardous material release, Network Outage	Cyber Attack, Security Breach, service provider failure, hardware/software failure or data loss
MINOR **Local Incident (within a Zayo site)** **Minor Incidents are managed internally by the team(s) usually on location. Events last less than 12 hours - no impact to business, customer, or employee.** **Notify IMT**	No fatalities. There may be inconsequential injuries Incident typically impacts single business unit Minimal to no disruption to critical processes or functions	Public health and safety not affected No off-site environmental impacts	MINOR repairs required - relocation not required Anticipated incident duration of 12 hours or less No surrounding community impact, but possible awareness Rarely creates local media interest	Minimal to no loss of technological assets Minimal to no repairs required Minimal to no disruption to critical processes / functions Minimal to no impact to products / customers
MODERATE **Local Incident** **(May affect more than one Zayo site in the same city or may be city, or county-wide incident - lasting 12 - 72 hours - NOT Catastrophic, however impacts may quickly escalate to a MAJOR event.** **Notify IMT, Activate Onsite Leaders**	May have serious injuries requiring hospitalization Incident usually impacts multiple business units Significant interruption of critical business process/functions Potentially significant impact to the corporation or brand.	Impact limited to facility, but has the potential for additional exposure or migrating off-site	Minor to moderate facility damage - partial relocation possible Substantial repairs required Anticipated incident duration of 12 - 72 hours May create local or regional media interest	Significant loss of technological assets or personal/confidential data Significant repairs required Significant interruption of critical processes/functions Disaster recovery plans invoked - relocation to alternate recovery site probable
MAJOR **Local or Corporate-wide Incident (may affect one or more Zayo locations, OR may be regional or national)** **All employees living or traveling to the area must be accounted for and the IMT activated. Impacts from these events usually last longer than 72 hours.** **Activate IMT**	Pandemic / Infectious disease outbreak Multiple Serious Injuries or Fatalities Severe impacts to multiple business units Severe impact to company, brand, or stockholder value Generates local, regional, or national media interest	Potentially impacts public health, safety & the environment or a large geographic area for an extended period of time	Severe to total facility damage - temporary or permanent relocation required Rebuilding required Anticipated incident duration of more than 72 hours Surrounding community impact and off-site actions required Incident creates a local, regional and/or national media interest	Severe or total loss of technological assets, significant loss of personal/confidential data Severe or catastrophic impact to specific product/customer Severe interruption of critical business processes/functions Severe or catastrophic impacts to the corporation All plans invoked - Relocation to alternate recovery site

6.1 Sample Incidents

INCIDENT ACTIVATION TRIGGERS	HUMAN	NATURAL	INFRASTRUCTURE	TECHNOLOGICAL
Example	Pandemic, workforce outage, terrorism, civil disorder, Corporate/Industry Incident	Severe weather - tornado, snow storm, flood, etc.	Power outage, building fire/explosion, hazardous material release, Network Outage	Cyber Attack, Security Breach, service provider failure, hardware/software failure or data loss
MINOR **Local Incident (within a Zayo site) Minor Incidents are managed internally by the team(s) usually on location. Events last less than 12 hours - no impact to business, customer, or employee.** **Notify IMT**	Food poisoning – office chili cook off - 30% of onsite workforce leave work for the rest of the day. Threatened workplace violence incident. Perpetrator is removed from the building. No injuries.	Building is evacuated due to area flooding and remains inaccessible (less than 12 hours)	Chemical fumes from construction causing physical symptoms in multiple employees – site is evacuated for remainder of the day. Small fire causing evacuation – quickly contained, damage is confined to the break room area. Water to the building is shut off due to a water main break. No water for 8 hours.	Corporate Data center is broken into and vandalized. No disruption to applications, backup data center works as planned. No data is lost and most of the equipment is able to be salvaged.
MODERATE **Local Incident (May affect more than one Zayo site in the same city or may be city, or county-wide incident - lasting 12 - 72 hours - NOT Catastrophic, however impacts may quickly escalate to a MAJOR event.)** **Notify IMT, Activate Onsite Leaders**	Rioting causes a city wide shut down. Access to the office is shut down for 24 hours. Workplace violence incident, serious, but non-life threatening injuries. Former employee files a harassment lawsuit against mid-level management. Local news coverage.	Blizzard shuts down roadways into the office for 2+ days	Statewide rolling blackouts affecting Core Locations Gas line explosion caused by Zayo personnel laying new fiber route. Manhole explosion while Zayo Personnel is splicing	Hackers steal confidential employee data Targeted DDoS attack affecting Tranzact
MAJOR **Local or Corporate-wide Incident (may affect one or more Zayo locations, OR may be regional or national) All employees living or traveling to the area must be accounted for and the IMT activated. Impacts from these events usually last longer than 72 hours** **Activate IMT**	Nationwide flu outbreak - 75% of workforce is affected. Zayo Executive(s) arrested for illegal activities, national news coverage Active Shooter situation. Multiple casualties	EF5 Tornado destroys core Zayo office and surrounding area. Major damage is caused to local infrastructure	Roof of a Core Zayo office collapses and the building is deemed untenantable and condemnedExtended Network Outage affecting Government Services with National News Coverage Network outage caused by vandalism affecting long haul fiber routes serving major city(s).	Virus erases Metasolv database and backups are not viable Hacker group ransoming Zayo confidential customer information for money.

7. Team structure and roles and responsibilities

The Incident Management organizational structure is patterned after the National Incident Management System/Incident Command System. It is meant to be flexible and scalable where only those roles needing to be activated are activated to keep the team small enough to manage the incident.

The nature of the Incident will dictate the type of subject matter experts (SME) involved. If an incident necessitates multiple SME teams, these teams will work separately but in tandem toward the same resolution. Each of these forums will designate a scribe to record details of these meetings and a representative to provide updates to the IMT Commander.

Role	Responsibilities
Frontline Employees	Identifying and reporting incidents that may need escalation. Provide detailed information about the incident.
Team Leaders and Managers	Monitor their teams' user base for any reports and communicate to the CMT.
Incident Response Analyst	Collect evidence pertaining to the incident and start bringing in stakeholders as needed. Activating communication with the CMT team, if the event impacts a large subset of users (internal or external).
Crisis Management Team	Decide if an event is potentially business impacting and whether notification to all or a subset of Zayo employees be sent via Crisis24 mass SMS and email.
Stakeholders	Identify team members that need to be involved in the incident.

8. IMT activation

Operations staff (including the NCC, Field Services, and Security, et al) should follow their already defined processes for notification and escalation, following the Chain of Command outlined in their own plans and procedures.

Technology staff should also follow their already defined processes for notification and escalation, following the Chain of Command outlined in their own plans, procedures and escalation documents.

8.1 When should the IMT activate the IMP?

This IMT should activate its Incident Management Plan (IMP) when an unexpected or disruptive event poses potential or actual impacts on operations, employees, customers, or assets. Activation is necessary for incidents that require a coordinated response to mitigate damage and restore normalcy. The IMP should be triggered for Moderate incidents (e.g., significant disruptions or safety risks) or Major incidents (e.g., severe, widespread impacts or media attention). The plan enables efficient communication, resource management, and recovery efforts, ensuring the organization responds effectively to minimize risks.

8.2 Who activates the IMT?

Escalation of events will occur and ultimately rise up to the executive level where each of the following people will make a judgment call as to whether the team should be activated.

The IMT may be activated for MODERATE events by one of these team members and should always be activated for MAJOR events:

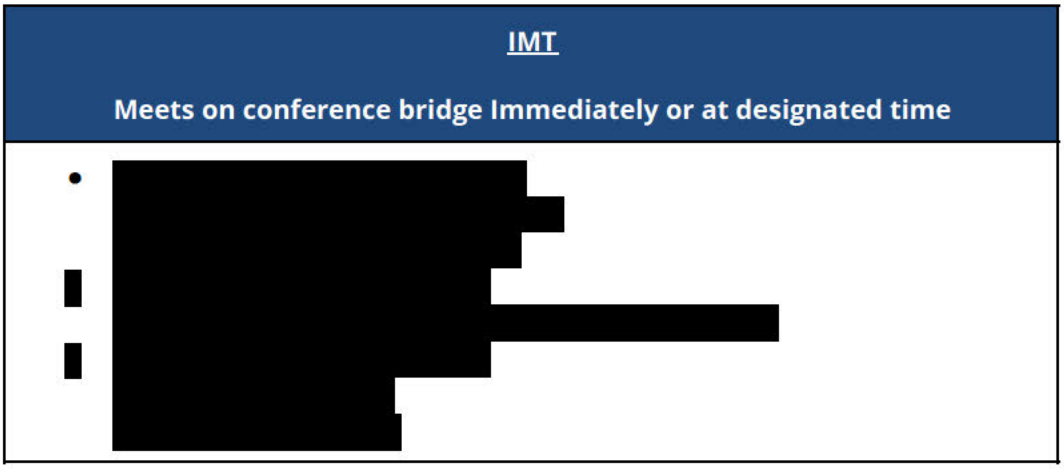
- CEO
- IMT Commander or Alternate
- PeopleOps Primary or Alternate Lead
- CFO or Alternate
- CIO or Alternate
- Operations Primary or Alternate Lead

8.3 How to activate

The IMT is activated when one of the above executives calls a zoom meeting (see below) via [redacted] with IMT IMMEDIATE ACTIVATION in the subject line and a short description of what's happening in the body of the email:

- What has occurred
- What is the location and specifics of the occurrence
- What documentation exists about the occurrence (ticket numbers, police report, etc.)
- What has been done thus far (additional parties already engaged)
- What outcome or outcomes need to occur

Team members should quickly join the meeting (if able) and stand by.



When the IMT is activated, this team meets virtually and in-person (as appropriate) to assess and triage the situation. It is up to the Commander whether to include the segment leaders (Incident Management Action Team or IMAT) or Site Safety Leaders in the IMT Meetings, depending on the incident.

- IMT members shall disseminate information to appropriate IMAT members immediately following the receipt of the Incident Action Plan.
- The IMT shall report status to the Incident Advisor during MODERATE and MAJOR events every two hours unless times are specified by the Commander. The Incident Advisor shall consolidate status and distribute or post online for the entire IMT.
- The IMT shall assist the Site Leaders as appropriate for assistance with funding, resources, and decisions.
- Participate in a daily IMT status briefings reviewing topics such as:
    - Assessment procedures
    - Impacts to customers, agents/partners, facilities, network, and workforce
    - Reporting requirements and forms
    - Safety and security issues
    - Any special insurance issues
    - Legal / Liability issues

9. Incident reporting

The Organization will appoint a Point of Contact (POC) responsible for managing communications with supervisory authorities and coordinating internal and external responses. The POC shall ensure that updates are timely, accurate, and consistent with regulatory requirements.

Any incident that has a significant impact on the continuity, availability, confidentiality, or integrity of customer critical services must be promptly reported, identified. and classified. This includes cyber incidents, data breaches, and operational disruptions. Reporting mechanisms include automated detection tooling, incident tickets using the [redacted] or contact Security directly via [redacted].

- The organization must notify the relevant supervisory authorities within 24 hours of becoming aware of a significant incident that meets the reporting thresholds of global laws and regulations
- Initial notification should include a summary of the incident, its impact, and the measures taken to mitigate risks
- Follow-up reports must be provided as further details become available, including the root cause, potential impact on services, and any corrective actions implemented

Notifications to supervisory authorities must include the following:

- A description of the nature and scope of the incident
- The estimated date and time of occurrence
- The immediate and potential impacts on the organization and its customers
- Details of the actions taken to manage and mitigate the incident
- Contact information for the designated POC within the Organization

All incident reports and notifications must be documented and retained for a minimum of five (5) years in accordance with data retention requirements. This documentation should be made available to supervisory authorities upon request for audit purposes.

Regular training shall be provided to employees and relevant stakeholders to ensure awareness of notification requirements and the appropriate procedures for reporting incidents.

10. Communications protocol

10.1 IMT notifications

Notifications may be sent to [redacted] as an FYI without activating the team. The subject or header line must be very specific if any action or follow up is needed.

As an example, for a medical emergency that occurred in Vancouver, the example email notification could read:

> **Subject:** "Incident Notification – Medical Emergency in Vancouver - No action required"
>
> **Body of the message:** "Employee Name suffered a heart attack today in the Vancouver office and was transported to the hospital and is expected to fully recover."

10.2 Internal communications

The Internal Information IMT member will release all messages to employees. The message should be reviewed at a minimum by the HR Lead and/or IMT Commander.

10.2.1 Emergency closures

Management will notify employees in the event of an office closure via chat, email, or phone call. If you suspect an office closure please check chatter prior to the beginning of your shift.

10.2.2 Management call trees

It is the responsibility of management to obtain and safeguard personal contact information for their direct reports. Notifications should be made to all employees, if possible and appropriate, about the status of the incident.

10.3 External communications

10.3.1 Media requests

The External Communications IMT member will respond to all media requests with a written statement (approved by the IMT Commander).

10.3.2 Financial, business, or reputation incidents

The Commander, Legal, and External Communications IMT Member need to be notified immediately during any incident that has the potential to damage Zayo's financial health, business, or reputation. The External Communications Plan will be initiated to mitigate the issue and protect Zayo's reputation as quickly as possible.

10.3.3 Security issues

The Chief Security Officer (CSO) must be notified of all security issues during a business disruption, including physical security, cybersecurity (loss or breach of data or information), or loss of hard copy records.

10.3.4 Federal agency requests

- The External Communications IMT member will work with Federal Agencies during natural disaster events for coordination efforts.
- The Legal IMT member will work with Federal Agencies during criminal investigations or security breaches.
- The Site Safety Team (SST) will work directly with Local Authorities during manned-site, Incident Management activities.

10.3.5 Data privacy breaches

Zayo's CSO will execute their plan for managing Data Privacy breaches when one occurs. The IMT and IMAT shall notify and escalate any privacy breach to the CSO. Because of the nature of personal information and the global reporting requirements for breach - any release and/or loss of personal information (PI) event shall be assessed as moderate to high initially as it needs involvement from IMT and Legal. The CSO shall determine reportability to Data Protection Authorities.

Note: Under General Data Protection Regulation (GDPR), we have 72 hours from incident discovery to report. External Communications shall be involved for public disclosure and specific customer notification.

11. Post incident review

The IMT & IMAT designated scribe(s) are encouraged to document the event(s) in real time via google docs to ensure accurate data is captured. This data is NOT to be shared outside of the IMT until the Commander has approved specific information to be shared. Following resolution of the Incident, the Commander will host a formal Post Incident Review to identify plan gaps, strengths, and training opportunities. An After Action Report (AAR) will be utilized to capture the specific items that need to be addressed as well as any necessary changes to the plan, processes, or procedures. These documents will be maintained and archived.

12. Acquisition or sale coordination

In the event of an acquisition or sale, the Enterprise Crisis Management Team (ECRT) will initiate a meeting with the seller's or buyer's crisis management team to align escalation paths and communication protocols. This coordination ensures a smooth transition and consistent response should an incident arise during this critical phase.

Key responsibilities during this phase include:

- Escalation Alignment: The ECRT will work with the counterpart crisis team to synchronize incident escalation processes and define clear lines of communication.

- Incident Coordination: The ECRT and the crisis team will collaborate to ensure that both parties are aware of their respective responsibilities and incident management procedures during the transaction.
- Plan Integration: Any pre-existing crisis plans from the involved parties will be reviewed and integrated, ensuring that there are no gaps in coverage for incident response.
- Ongoing Communication: Regular check-ins will be scheduled throughout the acquisition or sale process to update both teams on any changes that may impact incident management.

This alignment will mitigate any potential risks, ensuring both parties are equipped to respond efficiently to any unforeseen disruptions.

13. Acronyms

Acronym	Definition
AAR	After Action Report
Alert	A notification or signal that draws attention to a specific condition or situation requiring awareness or potential action.
CCP	Crisis Communication Plan
CMT	Crisis Management Team
ECRT	Enterprise Crisis Management Team (ECRT)
ERT	Emergency Response Team
Event	Any observable occurrence or activity that is significant within a particular context, whether planned or unplanned.
IMAT	Incident Management Action Team
IMP	Incident Management Plan
IMT	Incident Management Team
Incident	An unexpected or disruptive occurrence that requires a response to address its potential or actual impact.
LT	Leadership Team
OSS	Operational Support Systems

Acronym	Definition
GDPR	General Data Protection Regulation
CRT	Crisis Management Team
SST	Site Safety Team

14. Related documents

The following policies and/or standards are referenced within this Plan or contain additional requirements for compliance:

- *Zayo Security Policy*
- *Acquisition or Sale of Facilities, Technology, and Services Standard*
- *Audits and Risk Management Standard*
- *Leadership and High Level Objectives Standard*
- *Operational and Systems Continuity Standard*
- *Privacy Protection for Information and Data Standard*
- *Technical Security Standard*

15. Validity and plan management

This Plan is valid as of the date in the change history. The owner of this Plan is the Security team, who must test and update the Plan at least once a year.