



## Incident Response and Business Continuity Procedure

### Revision History

| Version | Date            | Change Number | Summary of Changes                                                                                            |
|---------|-----------------|---------------|---------------------------------------------------------------------------------------------------------------|
| 1.0     | 24 October 2025 | 001           | Initial creation and adoption of PCI-DSS Level 4 aligned Incident Response and Business Continuity Procedure. |
| 1.1     | —               | —             | —                                                                                                             |

### Document Review

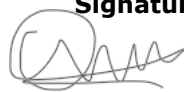
**Date of Next Scheduled Review:** April 2026

**Responsible Department:** Security & Compliance

### Distribution

| Name                      | Title                             |
|---------------------------|-----------------------------------|
| Preston Obadan            | Chief Executive Officer           |
| Oleksii W.                | Chief Security Compliance Officer |
| Kevin Kegera              | Chief Commercials Officer         |
| Departmental Heads        | All Divisions                     |
| Managed Service Providers | Where Applicable                  |

### Approval

| Name         | Position                          | Signature                                                                            | Date       |
|--------------|-----------------------------------|--------------------------------------------------------------------------------------|------------|
| Oleksii W.   | Chief Security Compliance Officer |  | 24/10/2025 |
| Kevin Kegera | Chief Commercials Officer         |  | 24/10/2025 |



## Table of Contents

1. Introduction
2. Incident Response Flowchart
3. Incident Detection and Notification
  - a. Incident Detection
  - b. Incident Notification
  - c. Recording Incident Details
  - d. Contacting the Incident Response Team Leader
4. Activating the Incident Response Procedure
  - a. Assemble Incident Response Team
  - b. Incident Response Team Members
  - c. Roles and Responsibilities
  - d. Incident Command Centre
  - e. Alternate Command Centre
5. Impact Assessment
6. Service Continuity Plan Activation
7. Incident Management, Monitoring and Communication
  - a. Communication Procedures
  - b. Means of Communication
  - c. Internal and External Communication
  - d. Media Communication
8. Ceasing Response Activities and Standing Down
9. Debrief and Post-Incident Review
10. Appendices (A-J)

## 1. Introduction

This document defines Orchestrate Global's **Incident Response and Business Continuity Procedure**, which guides coordinated action during any **disruptive event or security incident** affecting the **Cardholder Data Environment (CDE)** or other business-critical operations.

The objective is to ensure swift containment, effective communication, and minimal service disruption while maintaining PCI-DSS compliance and data protection obligations.



## Objectives

- Provide a structured framework for responding to disruptive or security incidents.
- Define who responds, how service continuity plans are invoked, and where operations relocate.
- Ensure timely internal and external communication during incidents.
- Maintain the security and integrity of cardholder and sensitive data.
- Fulfill legal and regulatory requirements.
- Document lessons learned for continuous improvement.

All personnel named in this document must keep a copy readily available.

Contact details will be verified three times a year, and updates sent to:

**service.continuity@orchestrateglobal.com.**

All information herein is processed under Orchestrate Global's **Data Protection Policy** and relevant data privacy laws.

## 2. Incident Response Flowchart

**Identify → Notify → Contain → Assess Impact → Activate Plans → Communicate → Recover → Review**

## 3. Incident Detection and Notification

### a. Incident Detection

Incidents may be detected via internal monitoring systems (SIEM, IDS/IPS, WAF), staff reports, customers, vendors, or emergency services. Early detection ensures rapid containment and mitigates data compromise.

### b. Incident Notification

The following authorized contacts may activate the Incident Response Procedure upon detection:

| Contact     | Department            | Email                                                                        | Availability |
|-------------|-----------------------|------------------------------------------------------------------------------|--------------|
| Team Leader | Security & Compliance | <a href="mailto:business@orchestrate.global">business@orchestrate.global</a> | 24/7         |



|                       |                  |                                                                            |               |
|-----------------------|------------------|----------------------------------------------------------------------------|---------------|
| Duty Manager          | Operations       | XXX                                                                        | After Hours   |
| HR Manager            | Human Resources  | <a href="mailto:hr@orchestrate.global">hr@orchestrate.global</a>           | 9–5, Mon–Fri  |
| Customer Service Lead | Customer Support | <a href="mailto:support@orchestrate.global">support@orchestrate.global</a> | 6–21, Mon–Sat |

## c. Recording Incident Details

Upon receiving an alert, record:

- Caller name and contact
- Date/time of report
- Incident type and location
- Whether emergency services are engaged
- Known injuries, fatalities, or data loss indicators
- Estimated scale and impact

## d. Contacting the Incident Response Team Leader

Use the **Initial Response Contact Sheet (Appendix A)** to escalate immediately.

If the Team Leader is unreachable, the initial responder is authorized to activate the procedure.

# 4. Activating the Incident Response Procedure

The Team Leader assesses whether activation is warranted based on:

- Danger to life or safety
- Significant business or operational disruption
- Potential cardholder data exposure
- Major reputational or legal impact

If criteria are met, the Incident Response Team (IRT) convenes at the **Incident Command Centre**.



## a. Assemble the Incident Response Team

The Team Leader will contact all IRT members (or deputies). The Incident Liaison proceeds to the incident site.

## b. Incident Response Team Members

| Role                | Primary Holder          | Deputy                 |
|---------------------|-------------------------|------------------------|
| Team Leader         | CSCO                    | IT Security Manager    |
| Team Facilitator    | Compliance Officer      | Operations Coordinator |
| Incident Liaison    | Risk Manager            | Site Supervisor        |
| Business Operations | CCO                     | Operations Manager     |
| Health & Safety     | Facilities Manager      | HSE Officer            |
| HR                  | HR Manager              | People Partner         |
| Communications      | Head of Corporate Comms | Marketing Lead         |
| Legal & Regulatory  | Legal Counsel           | Compliance Lead        |

(Contact details listed in **Appendix A.**)

## c. Roles and Responsibilities

**Team Leader:** Directs the response, authorizes activation, and acts as final decision authority.

**Facilitator:** Coordinates communications, logs activities, and supports operational logistics.

**Liaison:** Assesses incident impact onsite and provides continuous situational updates.

**Business Ops:** Evaluates service impact and customer dependencies.

**HSE:** Ensures safety compliance and emergency coordination.

**Communications:** Manages all internal/external information releases.

**Legal:** Advises on regulatory duties and reporting obligations (e.g. PCI-DSS, Central Banks, GDPR).

## d. Incident Command Centre

**Location:** \_\_\_\_\_

**Access:** Main entrance (8:00–17:30); after-hours access via Facilities Duty Manager (contact: +1 646 631 6118).

**Facilities:**

- Workstations, network access, secure storage



- Telephones, fax, projector, radio
  - PPE equipment, flashlights, stationery
- Parking:** Public lot available 24/7 opposite the building.

## e. Alternate Command Centre

If the primary site is inaccessible, operations will relocate to: [Insert alternate site details].

## 5. Impact Assessment

Upon assembly, the IRT conducts an **impact assessment** covering:

- Incident cause, duration, and scope
- Systems and infrastructure affected
- Cardholder or personal data exposure
- Business unit and customer impact
- Service and production effects
- Regulatory or legal exposure

Document findings using **Appendix B – Incident Impact Log**.

## 6. Service Continuity Plan Activation

Once the impact is clear, activate the relevant continuity plan(s):

| Document Ref | Plan Title                     | Description                                       |
|--------------|--------------------------------|---------------------------------------------------|
| Plan001      | Loss of Building A Access      | Relocate core functions to alternate site         |
| Plan002      | Loss of Primary Server Cluster | Restore from warm recovery backup                 |
| Plan003      | CDE Compromise                 | Isolate systems, invoke PCI-DSS forensic protocol |

Record activated plans using **Appendix C – Plans Activated Form**.



## 7. Incident Management, Monitoring and Communication

### a. Communication Procedures

Effective communication is essential during response and recovery.

#### i. Means of Communication

Primary: Landline and mobile phones

Secondary: Radio or secure messaging if networks fail

Email: Only via pre-approved encrypted channels

#### ii. Communication Guidelines

- Stay calm, concise, and factual.
- No speculation or unverified statements.
- Refer all external inquiries to the Communications IRT member.
- Document all interactions (Appendix E – Message Log Form).

#### iii. Internal Communication

Main command line: +1 646 631 6118 (8 incoming channels).

All internal messages should exclude confidential details unless verified secure.

#### iv. External Communication

External messages (clients, regulators, vendors) require CSCO or CEO approval.

Maintain a log of all contacts in **Appendix G – External Contacts**.

#### v. Communication with Media

Only authorized spokespeople may engage media.

Media statements must:

- Be legally reviewed
- Exclude personal data
- Reflect factual updates only

**Spokesperson**

**Role**

**Incident Scale**



|          |                         |        |
|----------|-------------------------|--------|
| Person A | IRT Communications      | Low    |
| Person B | Head of Corporate Comms | Medium |
| Person C | CEO                     | High   |

## 8. Ceasing Response Activities and Standing Down

The Team Leader declares stand-down when:

- The situation is stabilized or resolved
- Service continuity plans are operational
- Regulatory reporting is complete
- Risk is within acceptable levels

Document stand-down activities and recovery status.

## 9. Debrief and Post-Incident Review

A **24-hour debrief** is conducted post-incident to validate accuracy of event logs and lessons learned.

A formal **Post-Incident Review** follows, producing a **Post-Incident Report (Form ISMS23008)** within 14 days.

Key outcomes include:

- Root cause analysis
- Preventive recommendations
- Policy and control updates
- Training and awareness enhancements

## 10. Appendices



- **Appendix A:** Initial Response Contact Sheet
- **Appendix B:** Incident Impact Information Log
- **Appendix C:** Services Affected & Plans Activated
- **Appendix D:** Activity Logging Form
- **Appendix E:** Message Logging Form
- **Appendix F:** Internal Contact Directory
- **Appendix G:** External Agency Contacts
- **Appendix H:** IRT Meeting Agenda
- **Appendix I:** Command Centre Map & Floor Plan
- **Appendix J:** Phonetic Alphabet Reference