UNIVERSITY OF SUSSEX

Incident Response Guidance – Draft (This version: September 2025)

1.0 Incident Definitions

1.1 Critical Incident – Operational Response - Bronze Command – RAG Status Green

A Critical Incident will require an urgent response by teams within Faculties and Professional Services as an expected part of their normal operations. Escalation will not be necessary to manage the response, and no additional resources will be required. The University's 24/7 primary responders will normally be the Security Team, who will work in collaboration with Student Wellbeing, Residential Life, SEF Support Services and the incident response teams of any affected Faculty or Professional Service. Incident response teams will have documented plans in place and know how to inform impacted stakeholders. Such incidents will be overseen by an Incident Manager, usually the most senior staff member on site during the initial response. The Senior Security Manager present will act as Bronze Commander during the response and will escalate if additional support and tactical co-ordination is necessary. The Business Continuity Plans of affected Faculties and Professional Services may need to be invoked to support the response and promote recovery.

Critical Incidents are unlikely to impact the wider University Community. Examples may include:

- an isolated incident involving harm or distress to an individual (on or off campus, UK or overseas)
- denial of access or damage to small part of a building with no ongoing hazard (single-room failure)
- short-term evacuation due to temporary safety cordon or alarm (shelter not required)

1.2 Significant Incident – Tactical Co-ordination - Silver Command - RAG Status Amber

A Significant Incident is likely to require a coordinated response to supplement the aforementioned operational arrangements. During a significant incident, there may be disruption affecting numerous Faculties and Professional Services and this is likely to impact upon the University community. The Incident Co-ordination Team will be convened to gather information about the incident, to co-ordinate response and recovery activities and provide updates for internal and external communications about the incident. The Chief Operating Officer* will act as University Silver Commander (*Chief of Staff in the COO's absence).

Significant Incidents are likely to impact the wider University Community. Examples may include:

- hazardous conditions on Campus (e.g. severe weather, disruptive protest, chemical spill)
- community incident causes significant concern/distress/hardship (e.g. natural disaster, unrest)
- IT or utility outage – widespread disruption lasting more than 4 hours

1.3 Major Incident – Strategic Management - Gold Command - RAG Status Red

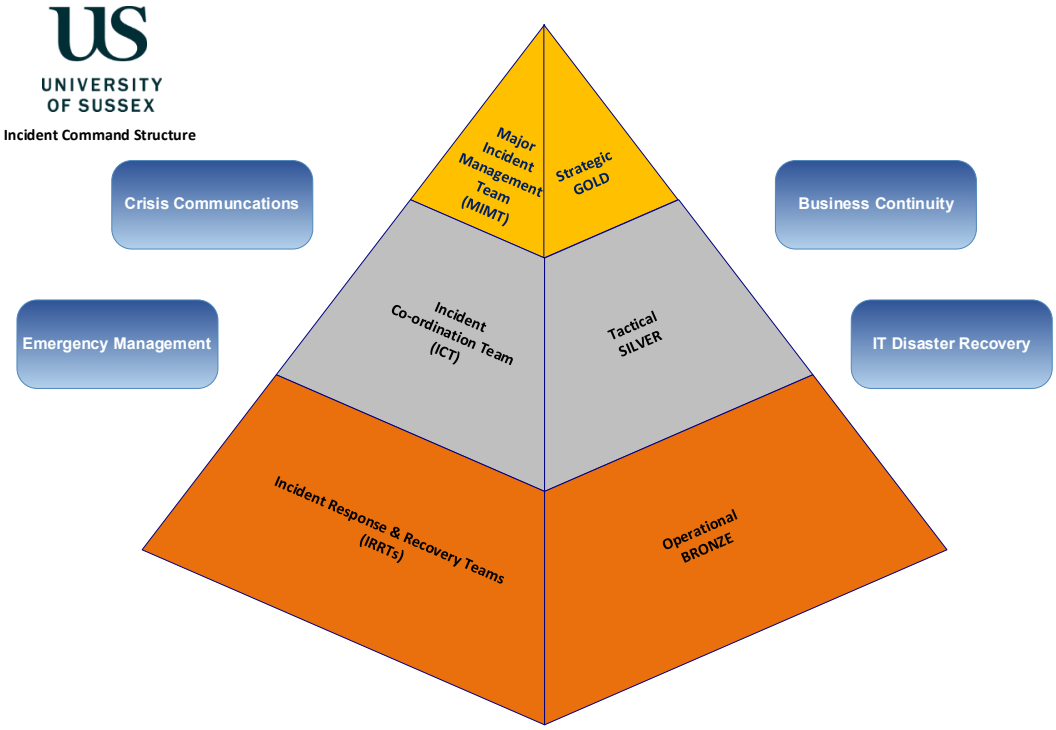
A Major Incident will have a more prolonged, University-wide impact requiring strategic management by the University's senior leadership. Major incidents are likely to cause prolonged disruption to the University's activities. The Vice Chancellor (or their nominated deputy) will act as the University's Gold Commander and the Major Incident Management Team (MIMT) will oversee decision-making throughout the response in order to secure resources that support recovery. The University's Crisis Communications Plan will be invoked to manage internal and external information about the incident and to monitor and respond to media coverage. Further details can be found in the University Business Continuity Plan.

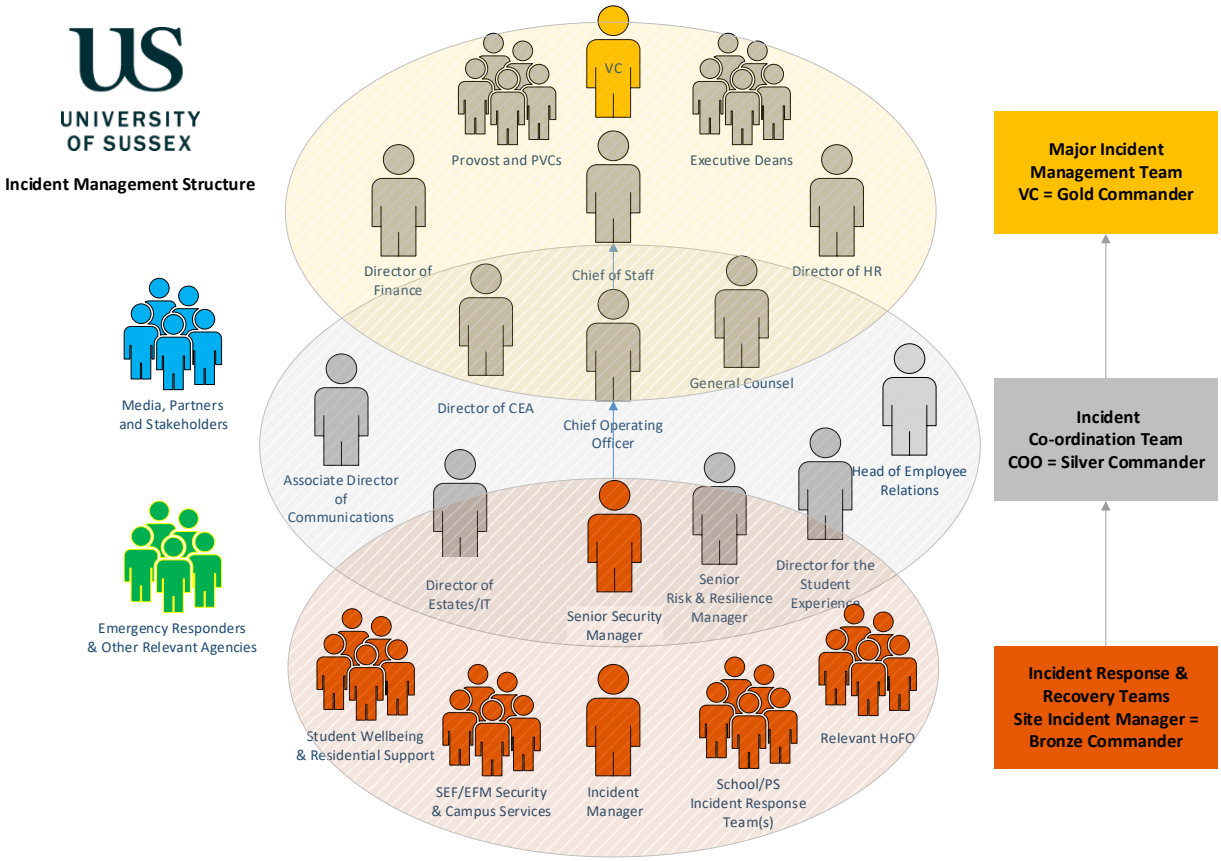
Major Incidents will cause significant disruption to the wider University Community. Examples may include:

- incident involving multiple casualties within the University's care (locally or overseas)
- explosion, fire or flood damages building(s), infrastructure and/or the environment
- large-scale evacuation due to life-threatening hazard (welfare support, emergency shelter)
- outbreak of life-threatening pandemic illness within the University community (e.g. Meningitis)
- utility outage/cyber incident causes prolonged disruption to University systems and activities

2.0 Command, Control and Communication

2.1 Incident Escalation – University Command Structure (Dependent on Scale of Incident – see Section 1)





During the initial response phase, the Bronze Commander will review the impact of the incident and if necessary, the overall management of the incident will be escalated to Silver and/or Gold Command.

2.2 Incident Escalation - Communication Flowchart

Incident Escalated by Operational Team(s) (Bronze Command)

- Escalation to Silver Command will be necessary when an incident is likely to have a significant impact on the wider University community (See Section 1), requiring additional resources and support. For example:
- unforeseeable - e.g. an urgent 'blue light' response requiring tactical management
- foreseeable - e.g. an Amber Severe Weather Warning covering the Brighton and Hove area is issued by the Met Office
- Action - Incident Manager to contact Silver Commander (COO) and provide SITREP (see Section 2.4)

Incident Coordination Team (Silver Command)

- Silver Team alerted via WhatsApp, Text Message, Email or MS Teams
- Silver Team Meeting Chaired by COO as Silver Commander - (MS Teams)
- Anknowledge incident, assess impact, prioritise safety and wellbeing and inform the University community
- Prepare initial holding statement and issue via appropriate channels
- COO to inform UET Members and escalate to Gold if a Major Incident

Major Incident Management Team (Gold Command)

- Major Incident declared - strategic management required
- University BC Plan invoked
- Major Incident Management Team meets - chaired by VC or Deputy VC
- Set strategic aim, consider risks and resource requirements to mitigate
- Consider strategy for recovery
- Agree frequency of future meetings and official statements

2.3 Incident Management Teams – Sample Meeting Agenda

1. Introductions and Team Wellbeing Check

2. Brief Description of Incident

- SITREP from operational responders - What do we know? What must we assume?
- Triage - Is this (or could this become) a Major Incident? Y/N

3. Set Objective

- High level – e.g. 'to protect life, and mitigate the impact of the incident'

4. Urgent Priorities for Immediate Action

- Initial holding statement to be agreed and issued (if required and not already done)

5. Note the Key Risks, Proposed Mitigation Measures and Agree Ownership

- Prioritise safety, wellbeing and community cohesion
- Consider reputational risks that may arise

6. Additional Resources Required

- Consider resource implications and impact on BAU
- Consider if there is a need to collaborate with external partner agencies

7. Communications Strategy

- Tone and timing of further updates
- Date/Time of Next Meeting (recommend 2-4 hours)

8. AOB

2.4 Situation Reporting (SITREP)

A SITREP should be a brief statement of fact to objectively describe what is currently known about the incident (e.g. what has happened and how we are responding). University responders should refer to the Red, Amber, Green (RAG) reporting system to indicate the current impact, as described in the table below:

RAG Status	Incident	Description of Impact	Response
Green	Critical	Isolated incident with negligible ongoing threat Short-term service disruption (< 1 day) Barely noticed by students, staff or stakeholders	Normal/ Operational (Bronze)
Amber	Significant	Numerous core activities suspended Medium-term service disruption (> 1 day) BC Plans may be invoked to support recovery	Tactical Co-ordination (Silver)
Red	Major	Loss of facilities, equipment or personnel Longer-term, University-wide disruption (2 days+) Activities suspended, prolonged recovery time	Strategic Management (Gold)

By adopting the SITREP (2.4) and METHANE (3.1) system, incident responders will be in a position to communicate consistently and coherently with other partners, such as members of the emergency services.

3.0 Incident Response – Action Card – Generic Guidance for operational staff responding to an incident

Detect and describe incident

- Initial notification - alert Security/emergency responders, start the incident log,
- Arrival at the scene, maintain safe distance and gather initial information about the incident
- Senior responsible person becomes Incident Manager/Bronze Commander
- Update other responders using METHANE report (see 3.1) - Is this a Major Incident?
- Escalate to Silver Command if signifcant impact and additional support is required
- Provide SITREP - describe what is happening, location, and who/what has been affected

Protect life, then property

- Prioritise safety at the scene and control access (if onsite), identify hazards and duty of care
- Dynamic risk assessment - monitor hazards, maintain safe distance and provide support
- Assess casualties and provide support to those affected, provide first aid as required
- Speak to witnesses - is anyone believed to be injured, trapped, in danger or missing?
- Evacuate people from affected areas as necessary and provide for their immediate welfare
- Set out safety cordon and confirm control point with emergency responders, if necessary
- Liaise with emergency services to safeguard critical assets and update senior commanders

Support those afftected

- Communicate with those directly affected at the scene (e.g. displaced people)
- Be prepared to evacuate a wider area, if advised to do so by emergency services
- Arrange temporary shelter for displaced people - a place of refuge with facilities, e.g. toilets
- Support people who have lost access to personal belongings or critical research materials
- Stand up services to deal with enquiries from concerned friends and relatives
- Overseas incidents - provide ongoing support and updates, examine options for repatriation
- Alert the Communications Team to warn and inform community and respond to enquiries

Mitigate impact of incident

- Invoke specific/local Emergency/BC Plans as necessary. If in doubt, report to line manager
- Notify/call-out designated staff and contractors (e.g. technicians, specialist advisers)
- Continue to maintain incident log of all noteworthy events and actions taken with timelines
- If escalated, provide updated SITREPs to Silver Command on a regular basis
- Brief Silver/Gold Command and confirm any urgent decisions and actions
- Communications Team to manage ongoing enquiries and messaging - agree timing and content of official statements
- Ongoing evaluation of impact and resource requirements
- Consider and develop recovery strategy

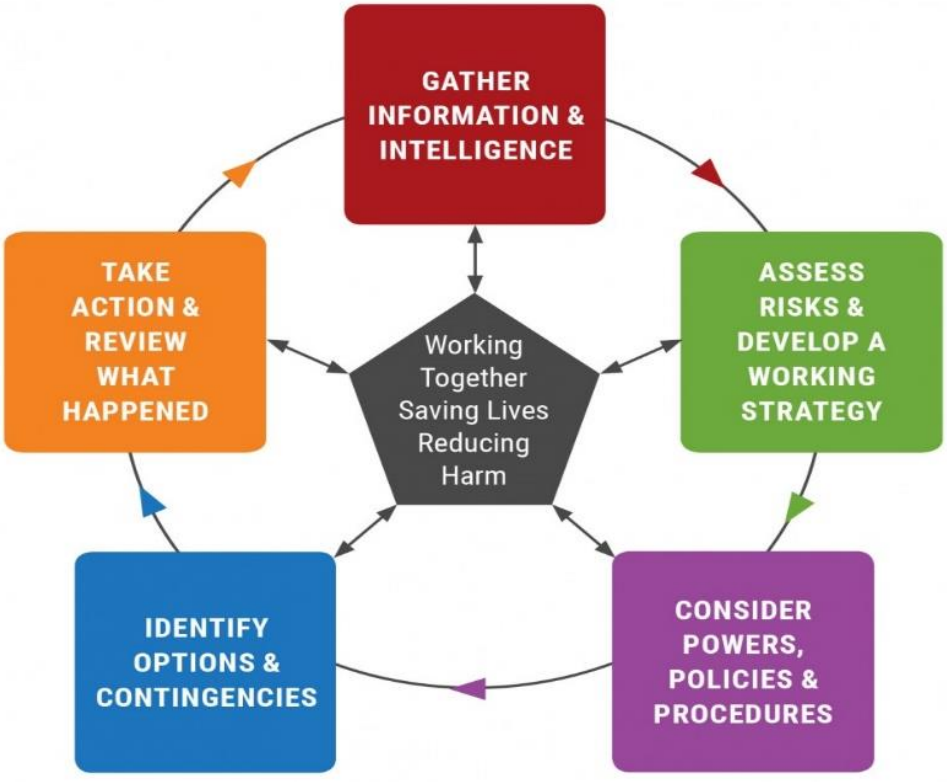
Plan for recovery

- Commence initial assessment of impact, losses, salvage activities and ongoing risks
- Agree and implement business recovery plans, priotitise essential activities
- Continue to inform staff, students and stakeholders about the impact and action taken
- Arrange de-brief to capture lessons learned
- Evaluate risk of future incidents and implement action to promote resilience
- Review incident response arrangements - resources
- Review business continuity and recovery plans - documentation

3.1 Incident Response – METHANE Reporting - shared situational awareness with other responders

M	MAJOR INCIDENT	Has a major incident or standby been declared? (Yes / No - if no, then complete ETHANE message)	*Include the date and time of any declaration.*
E	EXACT LOCATION	What is the exact location or geographical area of the incident?	*Be as precise as possible, using a system that will be understood by all responders.*
T	TYPE OF INCIDENT	What kind of incident is it?	*For example, flooding, fire, utility failure or disease outbreak.*
H	HAZARDS	What hazards or potential hazards can be identified?	*Consider the likelihood of a hazard and the potential severity of any impact.*
A	ACCESS	What are the best routes for access and egress?	*Include information on inaccessible routes and rendezvous points (RVPs). Remember that services need to be able to leave the scene as well as access it.*
N	NUMBER OF CASUALTIES	How many casualties are there, and what condition are they in?	*Use an agreed classification system such as 'P1', 'P2', 'P3' and 'dead'.*
E	EMERGENCY SERVICES	Which, and how many, emergency responder assets and personnel are required or are already on-scene?	*Consider whether the assets of wider emergency responders, such as local authorities or the voluntary sector, may be required.*

3.2 Incident Response – Emergency Services Joint Decision Model – aide memoire



3.3 Incident Response – General Principles

3.3.1 Gather and Share Information

- What has happened and how are we responding? Is this a Major Incident?
- Senior Security Manager (Bronze) to note the initial scale of the incident (SITREP).
- Start incident log. Note the time of any action taken and decisions made.
- Who should be informed as a priority at this stage? Is Escalation necessary?
- If yes, alert the COO (Silver Commander), if necessary via relevant Director.

3.3.2 Risk Assessment

- Preserve life – safety and welfare check to identify any immediate hazards or threats.
- Assess the initial impact of the incident and how the effects may be mitigated.

3.3.3 Consider Policies and Procedures - Establish Command and Control

- Establish if incident is within scope of existing plans and procedures, be prepared to adapt.
- Determine if there is a need for technical expertise and strategic decision-making.
- Liaise with any emergency responders and agree location of cordons and control points.
- Notify key any other personnel and stakeholders as necessary, including out-of-hours.

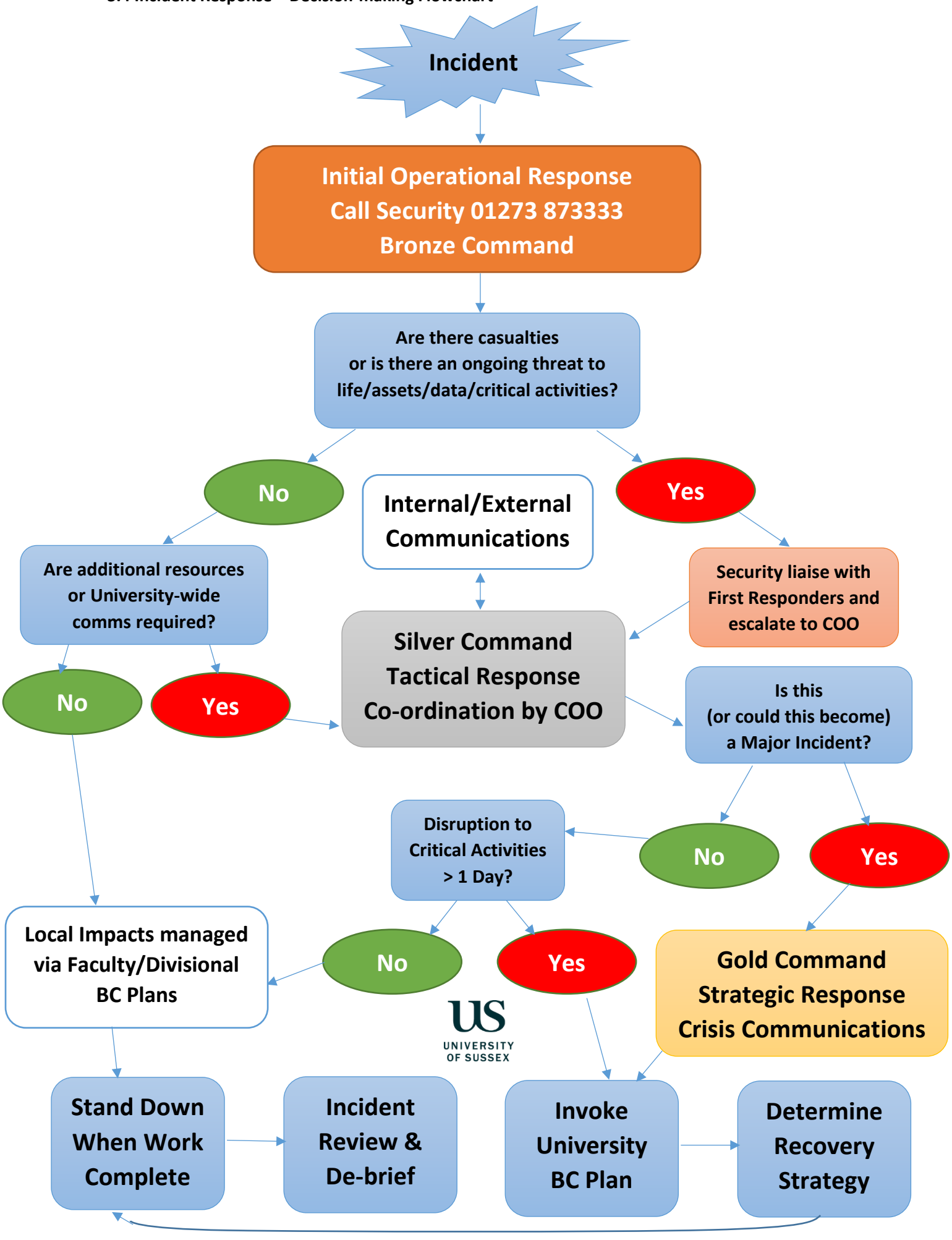
3.3.4 Objective Setting

- Prioritise the safety and welfare of people involved.
- Provide support to those affected, including concerned friends and family members.
- Identify any other urgent issues for immediate action e.g. scale of damage, disruption etc.
- Consider response capabilities and secure additional resources that will support recovery.
- Commence work with insurers to assess losses and to advise on level of cover.

3.3.5 Establish Communications Strategy

- Quickly acknowledge what has happened and inform the University community.
- Manage the initial surge of enquiries and the flow of information.
- Monitor media coverage and provide regular updates to all stakeholders.
- When appropriate, provide further details of the ongoing response and recovery efforts.

3.4 Incident Response – Decision-making Flowchart



4.0 Post Incident Review and Debrief

After the repsonse to the incident, a post-incident review should take place to provide assurance that the University has returned to 'business as usual' and to identify any lessons that have been learned.

Incident Response and Business Continuity Plans should include a 'review' section to ensure an assessement is undertaken after the event to establish why it happened, capture lessons learned to enhance future response arrangements and if possible, to prevent the recurrence of the most significant impacts.

Incident Response plans should be reviewed following any significant incident to incorporate any changes or improvements generated during the de-brief process. Where there is wider learning from an incident, these will be communicated to the University's Faculties and Professional Services through the Operational Resilience Working Group to ensure relevant plans have been updated.

5.0 Documentation for Reference – University Incident Response Plans

The following documents contain detailed procedures for responding to incidents:

5.1 University Business Continuity Plan – owned by COO, prepared by GCGC

- Procedures and guidance for responding to major incidents (on or off campus).
- Complements IT Continuity/Recovery Plans and Estates and FM BC Plans.
- Provides framework, templates and guidance for developing local BC Plans in Faculties and Professional Services.

5.2 Specific Incident Response Plans

- Campus Security/Emergency Response and Evacuation Plans – owned by EFM.
- Severe Weather Response Plan – owned by EFM.
- Power Outage BC Plan – owned by EFM.
- Cyber/IT Incident Response, Recovery and Continuity Plans – owned by ITS.
- Infectious Diseases Response Plan – owned by DSE.
- Protocols for Student Death/at Imminent Risk – owned by DSE.
- Global/Community Incident Response Protocol – owned by CEA/GCGC.
- BC Plans for Industrial Action, Protests and Demonstrations – owned by GCGC.
- BC Plans for critical activities such as Graduation, Open Days and Clearing – owned by CEA.
- Specific Faculty/School/PSD Incident Response and BC Plans* – owned by relevant Faculty/School/PSD.

** where applicable, to include local arrangements and escalation procedures for responding to incidents affecting students/staff who are studying/working overseas on behalf of the University.*

5.3 Crisis Communications Plan – owned by CEA

- Procedures for managing internal and external communications to warn and inform the community during a significant or major incident.