**Appendix 2 – Stages of Critical Incident Management**

|  |  |
| --- | --- |
| **Preparedness** | * Assess and treat disruption-related risk; understand institutional critical services; underpinning systems, processes, resources, and their interdependencies; identify and minimise vulnerabilities.
* Undertake continuous improvement of capability, including governance, delivery and people expertise.
* Develop plans, guidance, and other arrangements for critical incident management.
* Rehearse, test and provide assurance on the critical incident management arrangements.
* Establish approaches for scanning and identifying early warning indicators
 |
| **Response** | * Emergency Control Organisation (ECO) response – attending to the safety of building occupants, for example through evacuation.
* Broader emergency response, including incidents on and off campus.
* Issues and crisis recognition and management response, attending to incidents of high potential impact, (i.e. other incidents that do not constitute an emergency).
* Adaptive and extended BAU response.
* Strategic and operational continuity.
 |
| **Recovery** | * Disaster recovery of data, IT and telecommunications.
* Strategic and operational recovery and resumption.
* Facilities recovery and restoration.
* People recovery.
 |
| **Lessons learned** | * Investigating the incident, including identifying influencing factors.
* Debriefing on the incident and the response.
* Identifying lessons and recommending improvement actions.
* Implementing and monitoring those improvement actions.
 |
| **Evaluation and Monitoring** | * Evaluating and reviewing information to assist in decision making to develop forward planning
* Monitoring the development of the incident, and the success of any responses and interventions. To track the implementation of agreed actions from the review of the incident.
 |