Emergency Management Plan and Operation Policy

Original author's name:	Pkkirisankar Jagannath
Most recent date:	February 22, 2023
Most recent version number:	v1.0
Process owner:	Program Director

Document History

Version	Date	Revised by	Description
v1.0	November 22, 2019	Pkkirisankar Jagannath	Original Draft
V2.0	June 15, 2020	Kulpreet Singh	Ratified Version
V3.0	February 22, 2023	Pkkirisankar Jagannath	Ratified Version

Designated document recertification cycle in days:	[Cycle 30 90 180 **365**]
Next document recertification date:	February 22, 2024

Introduction

The Emergency Management Plan sets out the arrangements for coordinated action by the **22nd Century Technologies** (the "Company") in response to an emergency. In addition, it provides information on activities the Company shall engage in to ensure preparedness in case of an emergency. The mandate for this plan is provided by the Company Emergency Management Policy.

In the context of this plan, an emergency is an event, or series of events, that can cause death or significant injuries to staff; or that can suspend business, disrupt operations, create significant physical or environmental damage, or threaten the Company's financial standing or public image.

The Company's main objectives in its initial response to all emergencies are:

- to protect human life and alleviate suffering, and, as far as possible, protect property and reputation, and
- to support the continuity of everyday activity and the restoration of disrupted services at the earliest possible time.

The Emergency Management Plan supports these objectives by providing a clear and organised response strategy supported by pre-defined response procedures. Procedures and roles in this plan align with the Coordinated Incident Management System currently in use by all emergency organisations across United States.

The Emergency Management Plan forms part of a framework that provides for appropriate risk management of serious incidents that may disrupt the operations of the Company. The Emergency Management Plan is supported by the Company Emergency Procedures (Flip Charts) issued to staff and departments.

After the initial response phase of an Emergency, if required, the Company's Business Continuity Policy, Plans and related procedures will ensure that essential functions continue during and after a State of Emergency.

Objective of Emergency Planning

- Provide for the safety, health, and welfare of the employees in the TSCTI HQ
- Mitigate or contain the incident and its effects.
- Preserve property and provide safe occupation of building.
- Manage communications and information.
- Continue essential services and operations.
- Collect and analyze information to support decision-making and incident action plans.
- Manage organization resources effectively in the emergency response and recovery.

- Restoring general office operations.
- Cooperate with other agencies.

Scope of Emergency Planning

As per FEMA's National Risk Index, the Fairfax Counties Hazard's Type and Risk Indexes are below:

Hazard Type	Expected Frequency
Avalanche	Not Applicable
Coastal Flooding	Relatively Low Score 46.5
Cold Wave	Relatively Moderate Score 80.8
Drought	Very Low Score 49.8
Earthquake	Relatively Low Score 83.3
Hail	Relatively Low Score 79.7
Heat Wave	Relatively Moderate Score 92.1
Hurricane	Relatively High Score 96.9
Ice Storm	Relatively Moderate Score 80.3
Landslide	Relatively Moderate Score 86.1
Lightning	Relatively Moderate Score 78.2
Riverine Flooding	Relatively Moderate Score 76.3
Strong Wind	Relatively High Score 98.1
Tornado	Relatively Low Score 59.7
Tsunami	Insufficient Data
Volcanic Activity	Not Applicable
Wildfire	Very Low Score 48.5
Winter Weather	Relatively High Score 94.1

TSCTI considers only High Score frequency Hazards as part of it's Emergency Planning and mitigation strategy for now. The Moderate Hazard categories are to be taken in to consideration of TSCTI's Emergency Management Plan by the end of 2024.

Key Emergency Planning and Response Groups

The following groups have key roles to play in preparing for, and/or responding to, a Company emergency:

Infectious Diseases Emergency Planning Group	A broad cross-functional group of Company staff and representatives from external agencies responsible for planning and advising on the Company's response to epidemics, pandemics and infectious disease outbreaks.

Strategic Emergency Management Group	The group of senior staff responsible for focusing on strategic issues and making high-level decisions during, and in the aftermath of, a State of Emergency.
Incident Management Team	The designated group of appropriately trained, skilled and experienced staff that are responsible for the operational management of emergencies in accordance with the Emergency Management Plan.
ITS Disaster Recovery Planning	The designated group of ITS staff responsible for preparedness and
ITS Disaster Recovery Team	The designated group of appropriately trained, skilled and experienced staff that are responsible for assisting the Incident

1. Preparing for an Emergency

To ensure the Company is prepared for an emergency, pre-emergency planning is essential. Certain groups, as specified below, have a key role in this. However, other areas of the Company are also required to plan for potential emergency disruptions and should be aware of the Emergency Management Policy and the Emergency Management Plan.

1.1 Oversight of preparedness activities

(a) The **Director of Risk, Assurance and Compliance** is responsible for undertaking appropriate operational planning at the functional level to ensure the successful implementation and maintenance of the Emergency Management Plan and related plans. This shall include ensuring that detailed and integrated operational planning is done by relevant areas of the Company so that the Company is well positioned to respond to an emergency and to quickly recover after such an event.

(b) The Director of Risk, Assurance and Compliance will:

i. review the current status of emergency planning and build upon existing work completed

ii. identify resources and expertise necessary to support the policy and plan

iii. identify and plan for the continuity of essential services both during and after an emergency (including a pandemic/epidemic), and ensure that continuity planning activities across Service Divisions are integrated, practical and reflect the needs of Academic Divisions, and

iv. provide ongoing briefings and progress reports to the Audit and Risk Management Committee, Health and Safety and Ethical Compliance Committee as necessary.

1.2 Review of the Emergency Management Plan

(a) The Emergency Management Plan shall be reviewed annually by the Director of Risk Assurance and Compliance. Review will include consultation with the Director of ITS, Emergency and Business Continuity Coordinator, and other parties as deemed appropriate. Outcomes from testing exercises (see 1.6 below) shall also be taken into account as part of the review.

(b) The Director of Risk Assurance and Compliance shall report the outcome of the annual review of the Emergency Management Plan to the Chief Operating Officer.

(c) Substantive changes to the Emergency Management Plan as a result of annual review require the approval of the HR-Manager.

1.3 Pandemic/epidemic preparedness

(a) The Infectious Diseases Emergency Planning Group, convened by the Sr. HR-Manager, will meet twice a year to review and update the Company's pandemic and epidemic planning arrangements.

(b) The Sr. HR-Manager will act as the focus for all information with regard to the threat of pandemic/epidemic. Regular assessments of the international and local situation in respect of disease threat will be provided to the Infectious Diseases Emergency Planning Group using information from international, national and local health organisations as necessary.

(c) Health and Safety Compliance, in consultation with Employee Health, will provide public health education to staff and Employees. They will communicate clear, consistent and appropriate information to the Company community about how to reduce the risk of individual exposure (cough etiquette, hand washing, staying away from crowds), the role and importance of quarantine, vaccinations available, the symptoms of illness and what to do if they occur (including how and when to seek care).

(d) Company and Life Services shall assist with the dissemination of public health information (see 1.3(c) above) to residents of Company-owned and affiliated accommodation.

(e) Service Division pandemic response plans will be developed and maintained. These response plans will cover continuity of essential services and identification of new services/activities that will be needed to address pandemic/epidemic specific issues.

(f) All Company departments should be aware of pandemic/epidemic issues relating to specific Company areas and functions, as detailed in Appendix C of this plan.

1.4 ITS Disaster Preparedness

(a) The ITS Disaster Recovery Team, convened by the Senior Manager IT Infrastructure, will meet twice a year to review and update the Company's ITS disaster recovery planning arrangements.

(b) The Senior Manager IT Infrastructure will act as the focus for all information with regard to any potential threats to IT infrastructure. Regular assessments of the international and local situation in respect of IT threats will be provided to the ITS Disaster Recovery Team using information from international, national and local IT and Government organisations as necessary.

1.5 Severe Weather and Hazard Preparedness

(a) Hurricane:

The nature of a hurricane provides for more warning than other natural and weather disasters. A hurricane watch issued when a hurricane becomes a threat to a coastal area. A hurricane warning is issued when hurricane winds of 74 mph or higher, or a combination of dangerously high water and rough seas, are expected in the area within 24 hours. Once a hurricane watch has been issued:

- Stay calm and await instructions from the Emergency Coordinator or the designated official.
- Continue to monitor local TV and radio stations for instructions.
- Collect drinking water in appropriate containers.

Once a hurricane warning has been issued:

- Be ready to evacuate as directed by the Emergency Coordinator and/or the designated official.
- Leave areas that might be affected by storm tide or stream flooding.
- Remain indoors and consider the following: - Small interior rooms on the lowest floor and without windows, - Hallways on the lowest floor away from doors and windows, and - Rooms constructed with reinforced concrete, brick, or block with no windows.

(b) Strong Wind

Stay calm and await instructions from the Emergency Coordinator or the designated official.

- Stay indoors!
- If there is no heat: - Close off unneeded rooms or areas. - Stuff towels or rags in cracks under doors. - Cover windows.
- Eat and drink. Food provides the body with energy and heat. Fluids prevent dehydration.
- Wear layers of loose-fitting, light-weight, warm clothing, if available.

(c) Cold Weather

Stay calm and await instructions from the Emergency Coordinator or the designated official.

- Stay indoors!
- Have extra winter coats
- Coordinate with HR and Admin for adequate hitting in the Office premises

Power outages are a common hazard during a winter storm. If you experience a power outage, contact office Admin or wait for further instruction until emergency Power Kicks in.

1.6 Emergency communications preparedness

(a) Where practicable, communications should be prepared in advance of an emergency event. The Communications Team, under the Direction of the Head of Communications, may prepare generic scripts, web messages, and other communications in preparation for a potential emergency.

(b) Current contact lists of key staff (including after-hours contact details) will be available via either the Emergency and Business Continuity Coordinator or the Proctor. Such contact information will be reviewed and updated at least every six months by the Emergency and Business Continuity Coordinator.

(c) All Company departments should have 'communication trees' and staff contact details to allow direct communication in case of emergencies.

1.7 Training

(a) Training is a key component to the effectiveness of the Emergency Management Plan and will be provided to all members of the Strategic Emergency Management Group and the Incident Management Team along with other key staff likely to be involved in the response to an Emergency.

(b) The Office of Risk, Assurance and Compliance will run training at least once a year. Training will cover:

i. the contents of the Emergency Management Plan
ii. the role of people managing the response to an emergency
iii. the key skills and knowledge required to manage an emergency response.
iv. simulation exercises.

(c) New staff with roles identified in the Emergency Management Plan will be individually trained during their induction into the Company.

1.8 Testing the Emergency Management Plan

(a) The Emergency Management Plan will be tested at least once a year to ensure:

i. that procedures work effectively
ii. that staff are aware of their duties and are prepared for an Emergency, and
iii. that systems are resilient and function correctly.

(b) The Office of Risk, Assurance and Compliance is responsible for:

i. ensuring the Emergency Management Plan is tested
ii. agreeing the exercise objectives and selecting an appropriate exercise format
iii. recording attendance, and
iv. overseeing the post-exercise improvement plan.

(c) When testing the Emergency Management Plan the exercise scenarios will be based on, though not limited to, the risks included in the Company Emergency Procedures (Flip Charts). The exercises will aim to simulate emergencies occurring at different times of the day, on different days of the week, and during various months of the year.

(d) The following crucial elements will be tested:

i. the contact list
ii. the activation process
iii. communications equipment
iv. setting up procedures, and
v. information and communications management.
Vi. Emergency drills

2. Alert Status

While some emergencies, such as a major earthquake, will strike without warning, other emergencies may be foreseeable and give some time for preparation, for example pandemic events or some types of flooding. In such cases, the Company may enter an Alert Status, for the purposes of monitoring, immediate planning, and communications to the Employees.

Alter Status activation shall be the responsibility of the Emergency and Business Continuity Coordinator (or his/her delegate), in consultation with the Director.

2.1 Alert Status activities

(a) During an Alert Status, the Incident Controller will assemble the Incident Management Team for planning discussions and to keep the HR-Manager updated on the development of events.

(b) During an Alert Status, Incident Controller, with the support of the Incident Management Team's Communications Team, shall be responsible for communications to the Company Employees (see section 5).

(c) In the event of an Alert Status relating to a pandemic or epidemic, the Sr. HR-Manager with the support of the Infectious Diseases Emergency Planning Group as appropriate, will assist the Incident Controller in making decisions about appropriate actions (see below).

(d) In the event of an Alert Status relating to a potential ITS disaster, the

Senior Manager IT Infrastructure, with the assistance of the ITS Disaster Recovery Team as appropriate, will assist the Incident Controller in making decisions about appropriate actions (see below).

2.2 Pandemic/Epidemic Alert Status adoption

(a) A Pandemic Alert Status will normally be adopted where:

i. there is very high suspicion of human-to-human transmission of the relevant illness overseas, or

ii. there is human-to-human transmission of the relevant illness overseas, or

iii. Australia and/or Singapore and/or China close their borders, as they have been identified as the main transit ports to United States from countries likely to be affected.

(b) An Epidemic Alert Status may be adopted as required, taking into account advice from the Ministry of Health, and other health and/or government organisations.

(c) Actions relating to a Pandemic or Epidemic Alert Status are detailed in Section 6 of this Plan (see particularly 6.1(e)).

2.3 ITS Disaster Alert Status adoption

(a) An ITS Alert Status will normally be adopted where:

i. there is very high suspicion of significant threats to IT overseas.

3. Declaration of a State of Company Emergency

When an event reaches a critical point, or threatens to reach a critical point, the HR-Manager may declare a State of Company Emergency.

3.1 Determining that an emergency justifies the declaration of a State of Company Emergency

(a) A State of Company Emergency shall be declared by the HR-Manager whenever an emergency occurs which cannot be handled by day-to-day operations and management. This will be upon receipt of information from the Emergency and Business Continuity Coordinator

Amongst the key factors for the HR-Manager to consider in making the declaration are:

i. whether it is a high impact event

ii. whether life and/or property are at risk

iii. whether a large area is affected (entire Company/city/region)
iv. whether outside emergency services are involved
v. whether the emergency is longer term (normally longer than one day), and/or
vi. whether the emergency is a serious health incident which could cause major disruption to Company employees and services.

(b) In a pandemic event, a State of Company Emergency will usually be declared at the point when human pandemic strain cases are identified within United States, and/or on the advice of Ministry of Health.

(c) In an epidemic event, the decision to declare a State of Company Emergency will take into account advice from the Health departments, and other health and/or government organizations.

(d) The principle of 'prudent over-reaction and rapid de-escalation' applies when making the decision to declare a State of Company Emergency. It is easier and usually more effective to scale down an over-reaction than it is to escalate an under-reaction.

3.2 Process for declaring a State of Company Emergency and activating emergency management processes

(a) The Incident Controller recommends to the HR-Manager that a State of Company Emergency be declared.

(b) The HR-Manager formally declares a State of Company Emergency.

(c) The Incident Controller advises the Communications Team, via the Head of Communications, that the HR-Manager has declared a State of Company Emergency.

(d) Staff in the Strategic Emergency Management Group and the Incident Management Team are released from their normal duties to take up their prescribed roles.

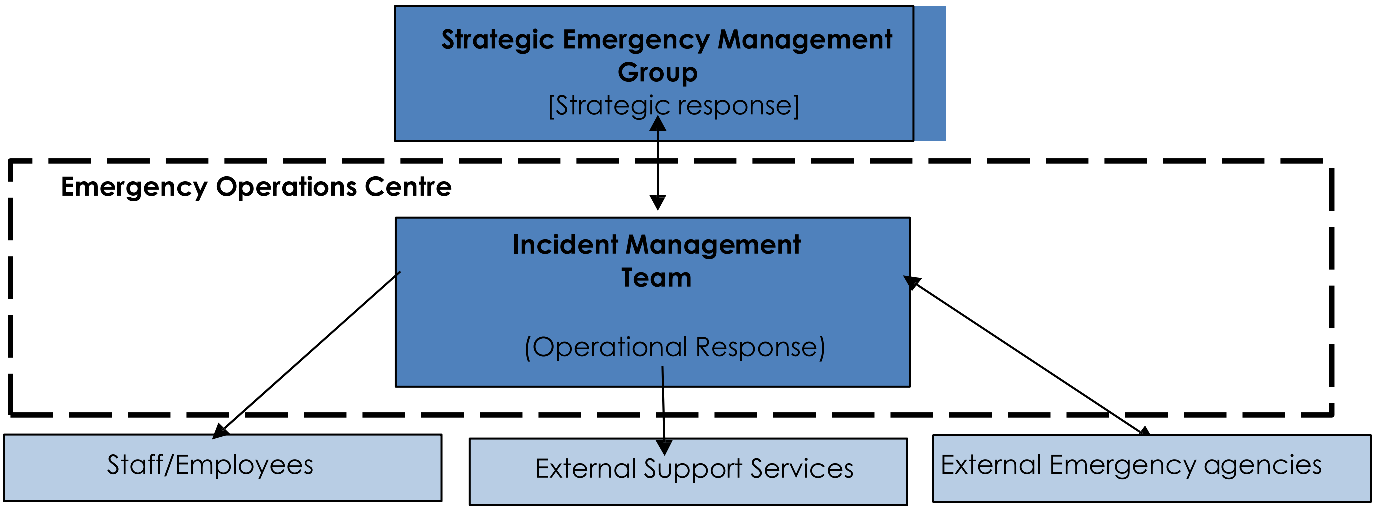
(e) The Communications Team takes all necessary steps to notify employees that a State of Company Emergency exists (further information is available in the Communications section of this Plan).

(f) The Incident Controller assembles the Incident Management Team and activates the Emergency Operations Centre at the respective Company. The EOC location will be determined at the time by the Incident Controller, based on the emergency type and location.

(g) The HR-Manager assembles the Strategic Emergency management Group in the Council Chamber in the Registry Building, or an alternative location if this is not available.

4. Response during a State of Company Emergency

During an emergency the Company shall use the US Coordinated Incident Management System (CIMS), with minor modifications to suit the Company, as its incident management model. This section provides information on the groups that shall coordinate the Company's response, using the following structure:


Strategic Emergency Management Group
[Strategic response]
Emergency Operations Centre
Incident Management Team
(Operational Response)
Staff/Employees
External Support Services
External Emergency agencies

4.1 The Emergency Operations Centre

(a) The Emergency Operations Centre (EOC) serves as the centralised facility in which the Incident Management Team will gather, check in, and assume their emergency response roles. The core of the Communications Team shall also be situated in the Emergency Operations Centre during a State of Company Emergency.

(b) Tactical and short-term response activities and work assignments in support of the on-scene field command will be planned, coordinated, and delegated from the Emergency Operations Centre.

(c) The Incident Management Team is comprised of a broad cross section of staff, selected for their expertise and the needs of the Emergency Operations Centre. The Incident Controller determines the appropriate level of activation and calls out the designated Incident Management Team members.

(d) When requested, designated EOC staff should report directly to the Emergency Operations Centre. If an EOC member is unsure whether to report, he or she should first contact the Company Watch on (+1) 6096453413 to determine when and where to report.

(e) The Office of Risk, Assurance and Compliance shall maintain a plan for the operation of the Emergency Operations Centre during an emergency.

4.2 The Incident Management Team

(a) The Incident Management Team is led by the Incident Controller and is responsible for the operational management of emergencies.

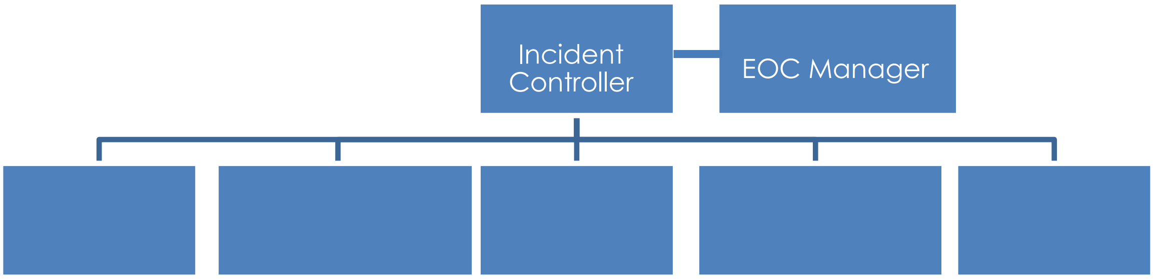
(b) The Incident Controller shall be:

i. the Emergency and Business Continuity Coordinator or other delegated authority

ii. the Senior Managers Client Services in US, or other nominee selected by the Manager and/or

iii. the Operations Coordinator.

(c) The Incident Management Teams will be comprised of selected staff within the Company and will utilise the following structure:



(d) The Incident Management Team shall be responsible for:

i. coordinating and managing the response to an emergency with the immediate focus on saving life and property
ii. taking immediate steps to prevent any further injury
iii. taking immediate steps to prevent further damage to property
iv. providing accurate and timely information to the Strategic Emergency Management Group.
v. providing support for any emergency service agency on Company, including provision of information or resources
vi. setting up, staffing and operating a welfare centre for staff and Employees as necessary, to be a source of information, personal services, counselling and support both during and after an emergency, and
vii. providing accurate information to the staff, Employees, about the emergency situation, via the Communications Team.

(e) Each shift of the Incident Management Team shall prepare an Incident Action Plan to record administrative details and instructions issued, and to provide a reference for managing the incident that can be easily picked up and acted upon by the incoming shift. For ongoing emergencies, 12 hours shifts (12 on, 12 off) are recommended.

(f) Individual role responsibilities within the Incident Management Team are detailed in Appendix A.

4.3 The Strategic Emergency Management Group

(a) The Strategic Emergency Management Group is led by the HR-Manager and is responsible for the strategic management of emergencies.

(b) The Strategic Emergency Management Group shall be comprised of the HR-Manager's Advisory Group and other senior staff as required:

- HR-Manager
- Deputy HR-Manager (Academic)
- Deputy HR-Manager (Research & Enterprise)
- Deputy HR-Manager (External Engagement)
- Chief Operating Officer
- Chief Financial Officer
- Director of Human Resources
- Head of Communications

(c) In the event that the HR-Manager is unavailable, the Strategic Emergency Management Group shall be chaired by one of the Deputy HR-Managers. In the unlikely event that none of the named executive staff are available, the Incident Controller will locate a Sr HR Manager who will assume the role until such time as one of the named staff are available.

(d) The Strategic Emergency Management Group shall be responsible for:

i. making and acting on decisions requiring the highest authority within the Company
ii. supporting the immediate actions of the Incident Management Team.
Iii overseeing communications with staff, Employees
iv. focusing on major strategic issues, and
v. through the Chief Operating Officer, overseeing business recovery and continuity.

(e) The Strategic Emergency Management Group will maintain key relationships with:

i. the Incident Management Team and the Communications Team
ii. the overall Company community (in the event of a major incident affecting the Company, information, direction and support will be required and must be made available in a relatively short period), and
iii. relevant external parties such as the DCC, Otago Polytechnic and the wider Company sector throughout the country (in the event of a major incident, support and backup services may be available through these links).

(f) Key roles and responsibilities within the Strategic Emergency Management Group are detailed in Appendix C.

4.4 External support

(a) External parties, including but not limited to the following, may provide support during an emergency:

- City or regional councils
- District Health Board hospitals and services
- Police
- Fire Service
- National services in a Civil Defence emergency
- Ministry of Health in a pandemic/epidemic emergency

5. Emergency Communications

This section provides additional information on how the Company will manage communications with staff, Employees during a State of Company Emergency. It is important that there is a clear process and one definitive source of truth during an emergency to enable clear communication and prevent the spread of incorrect or confusing information.

Parts of this section are also relevant to an Alert Status (see section 2).

5.1 Information control

(a) The Communications Team is responsible for all internal and external communications during a State of Company Emergency, with the exception of announcements from the HR-Manager (or delegate), which shall be drafted in consultation with the Head of Communications.

(b) During a State of Company Emergency the Communications Team may approve the use of pre-approved and pre-scripted messages in communications about the emergency (e.g. via the Company Contact Centre). All other messages will be approved by the Incident Controller prior to release.

(c) Information released through the Communications Team serves as the only information about the Emergency which Company staff should share with internal and external audiences. Company staff who wish to share other information must first consult the Head of Communications.

(d) Clauses 5.1(a) to (c) above apply to information pertaining to a pandemic/epidemic or other potential emergency event during an Alert Status.

(e) During a State of Company Emergency, the Communications Team will monitor TV and radio, internet news sites and social media sites to identify and correct substantive rumours and misinformation.

(f) In a rapidly unfolding crisis, or an event occurring during non-business hours, the Police may initiate urgent communications independently. The Police are responsible for answering queries related to police activities, including announcements of loss of life.

5.2 Emergency communication channels

(a) During a State of Company Emergency or Status Alert, the Company website will be the primary tool for communication about the emergency, via the main homepage and mirrored information on the homepages for the employees. Alternative communication channels may be used if internet access is disrupted.

(b) Staff, Employees will be directed to the Company website for updates about the emergency.

(c) The following channels may also be used for communications during or after a State of Company Emergency or Status Alert (subject to the direction of the Communications Team):

System	**Responsibility**
All-staff email	Incident Management Team - Communications
All-staff voicemail	Incident Management Team - Communications
All-Employee text	Incident Management Team - Communications
All-Employee email	Incident Management Team - Communications
Company website	Incident Management Team - Communications
Company screens	Incident Management Team - Communications
Emergency telephones and/or PA system	Incident Management Team - Operations
Email media releases	Incident Management Team - Communications
Radio/television (including Radio One broadcasts)	Incident Management Team - Communications
Social media (including Facebook and Twitter)	Incident Management Team - Communications

5.3 Communications responsibilities outside the Communications Team

(a) Information Technology Services has overall responsibility for the communication and data systems used for emergency communications.

(b) Human Resources is responsible for ensuring that all staff have accurate personal information recorded in the payroll system, and for supporting ITS with respect to the use of any HR systems that are required for Emergency communication needs.

(c) The Communications Team is responsible for liaising with all to assist in disseminating information that has been provided by the Incident Management Team, to Company Employees using Radio, social media, the Critic web site and other channels.

(d) Ask staff within Shared Services will:

i. field incoming calls from staff, Employees, and respond based on a script provided by the Communications Team
ii. ensure that all media enquiries are redirected to the communications Team, and
iii. record rumours and misinformation from the and pass that information on to the communications Team.

(e) Additional personnel may be required to provide a variety of services as necessary and as requested by the communications Team, including posting web updates, press conference set-up, field monitoring, handling calls from Employees' families and fielding other incoming calls and emails.

7. Recovery

After the initial phase of an emergency, operational responsibility shifts from the Incident Controller to the Recovery Manager (the Chief Operating Officer), who will coordinate and facilitate recovery activities.

The Company’s Business Continuity Policy, and business continuity plans for individual areas, will then become the key documents as the Company seeks to minimise disruption and restore operational activities as soon as possible following the emergency.

Glossary

Alert Status	A pre-emergency status relating to an increased risk of a potential emergency, including the risk of an epidemic, pandemic and/or infectious disease outbreak. During an Alert Status the Company may communicate information and carry out precautionary measures.
Coordinated Incident Management System	A system adopted by all emergency organisations in United States and internationally for implementation at times of emergencies.
Emergency	An event, or series of events, that can cause death or significant injuries to staff, Employees ; or that can suspend business, disrupt operations (i.e. critical infrastructure/utilities/IT network), create significant physical or environmental damage, or threaten the Company's financial standing or public image.
Emergency Management Policy	The overarching Company policy which specifies how the Company shall respond to significant emergency situations and related staff responsibilities. The Emergency Management Policy underpins the more detailed Emergency Management Plan.
Epidemic	A widespread occurrence of an infectious disease. In terms of this plan it is primarily used to refer to a United States outbreak.
Incident Controller	The Incident Controller leads the operational response to an emergency, via oversight of the Incident Management Team.

Incident Management Team	The designated group of appropriately trained, skilled and experienced staff that are responsible for the operational management of emergencies in accordance with the Emergency Management Plan.
ITS Disaster Recovery Team	The designated group of appropriately trained, skilled and experienced staff that are responsible for planning and advising on the Company's response to an ITS disaster and assisting the Incident Management Team with the response to the disaster.
Communications Team	The team responsible for internal and external communications during an emergency, comprising communications staff under the direction of the Incident Controller.
Medical Officer of Health	A designated public health official appointed for a health district under the Health Act.
Pandemic	A widespread occurrence of an infectious disease occurring across multiple countries.
Infectious Diseases Emergency Planning Group	A broad cross-functional group of Company staff and representatives from external agencies responsible for planning and advising on the Company's response to epidemics, pandemics and infectious disease outbreaks. The group is convened by the Sr. HR-Manager(Health Sciences) or their delegate.

Recovery Manager	The person responsible for facilitating and coordinating the medium and long term recovery activities of the Company after an emergency. The Recovery Manager at the Company is the Chief Operating Officer.
State of Company Emergency	A declared status that indicates that an emergency cannot be managed via normal operations, and which activates provisions in the Emergency Management Plan.
Strategic Emergency Management Group	The group responsible for focusing on strategic issues and making high-level decisions during, and in the aftermath of, a State of Company Emergency. The group is comprised of senior staff and is led by the Sr. HR Managers.
HR-Manager	For the purposes of this plan, references to the HR-Manager also cover any Acting HR-Manager.

Appendix A - Incident Management Team Role Descriptions

Incident Controller

Role
Takes responsibility during an emergency and leads a coordinated response. The Incident Controller's primary concerns are ensuring the response gets underway in a timely fashion and continues without seriously faltering.

Supervises
The staff member in charge of Operations, Logistics, Planning and Intel, Health and Safety, and Communications.

Reports To
Strategic Emergency Management Group

Key Objectives

- Direct the Incident Management Team
- Protect life
- Protect Company property
- Relieve distress
- Provide support for the most expedient return to normal operations

Responsibilities

- Assume control of the incident and of all Company's response capabilities under the delegated authority of the HR-Manager
- Assess the situation
- Decide on the scale of the response and activate either partial or full incident management team involvement
- Establish Coordinated Incident Management System management structure
- Appoint, brief and task Incident Management Team
- Activate the Emergency Operations Centre and other facilities as required
- Plan future staff requirements and changeovers
- Maintain safe practices
- Record decisions, actions, and other activities
- Regularly brief the Strategic Emergency Management Group
- Contribute to post-incident debrief

Key Relationships

- Strategic Emergency Management Group (SEMG)
  - The incident Controller provides primary briefings to the SEMG.
  - The Incident Controller identifies major resource requests (including human), policy issues and matters arising from the incident that the SEMG must consider.
- Operations (Incident Management Team)
  - The Operations Manager directs the operational response to

the Emergency and provides regular situation reports and updates to the Incident Controller.

- Logistics (Incident Management Team)
  - Logistics provides advice on resource availability, capability and sustainability to assist the Incident Controller in formulating his/her strategy.
- Planning and Intelligence (Incident Management Team)
  - Planning and Intelligence provides predictions of incident development to assist the Incident Controller in developing realistic goals and priorities for the incident response.
  - Planning and Intelligence provides regular (collated from all sources) situation reports to the Incident Controller.
  - Planning and Intelligence administers the production of each successive version of the Incident Action Plan and provides it to the Incident Controller for their approval.
- Health and Safety (Incident Management Team)
  - Health and Safety advises the Incident Controller on the safe implementation of the Incident Action Plan.
  - Health and Safety advise on the external authority notification and investigation processes.
- Communications Team
  - Communications Team develop communication strategies and key messages and provide these to the Incident Controller for their approval.

Operations Manager

Role

Directs response operations. The Operations Manager may often need to leave the Emergency Operation Centre and observe/direct response operations and resolve operational problems. This avoids whole Incident Management Team involvement in the details of frontline activity.

Supervises

The staff members within the Operations Team.

Reports To

The Incident Controller.

Key Objectives

- Protect life
- Protect Company property
- Relieve distress
- Provide support for the most expedient return to normal operations
- Direct the Operations Section

Responsibilities

- Get to the Emergency Operations Centre as soon as possible
- Obtain briefing from the Incident Controller
- Record decisions, actions and other activities
- Determine the Operations management structure

- Appoint, brief and task staff
- Manage and supervise operations at the incident
- Establish Staging Areas (Logistics provides and Operations manages this function)
- Deploy and manage resources in the field
- Develop and implement response tactics
- Review resource needs
- Resolve operational problems
- Ensure safety and welfare of personnel
- Participate in Incident Action Plan development meetings
- Report significant events

Key Relationships

- Incident Controller
  - The Incident Controller provides overall direction, priorities and tactics.
  - The Operations Manager buffers the Incident Controller from minor operational problems.
  - The Operations Manager is the ‘eyes and ears’ of the Incident Controller at the front line.
  - The Operations Manager develops response tactics and advises the Incident Controller.
- Logistics (Incident Management Team)
  - Operations requests resources from Logistics.
  - Logistics provides resources and tracks them until they are taken over during response operations by Operations.
  - Logistics assists Operations to manage resources to sustain operations functions.
- Planning and Intelligence (Incident Management Team)
  - Planning and Intelligence provides predictions of incident development to assist the Operations Manager to develop sustainable tactics.
  - Planning and Intelligence highlights possible problems and opportunities to Operations. Operations provides regular situation reports to Planning and Intelligence to inform the Incident Action Plan.
- Health and Safety (Incident Management Team)
  - Health and Safety works with Operations to ensure that operations are as safe as possible.

Communications Manager

Role

Directs communication operations.

Supervises

The staff members within the Communications Team.

Reports To

The Incident Controller.

Key Objectives

- Protect life

- Protect Company property
- Relieve distress
- Provide support for the most expedient return to normal operations
- Direct the Communications Team

Responsibilities

- Get to the Emergency Operations Centre as soon as possible
- Obtain briefing from the Incident Controller
- Record decisions, actions and other activities
- Determine the Communications management structure
- Appoint, brief and task staff
- Manage and supervise communications at the incident
- Deploy and manage resources in the field
- Develop and implement communication strategies
- Review resource needs
- Resolve communication problems
- Ensure safety and welfare of personnel
- Participate in Incident Action Plan development meetings
- Report significant events

Key Relationships

- Incident Controller
  - The Incident Controller provides overall direction, priorities and tactics.
  - The Communications Manager buffers the Incident Controller from minor communication problems.
  - The Communication Manager develops communication strategies and advises the Incident Controller.
- Logistics (Incident Management Team)
  - Communications requests resources from Logistics.
  - Logistics provides resources and tracks them until they are taken over during response operations by Communications.
  - Logistics assists Communications to manage resources to sustain operations functions.
- Planning and Intelligence (Incident Management Team)
  - Planning and Intelligence provides predictions of incident development to assist the Communications Manager to develop sustainable tactics.
  - Planning and Intelligence highlights possible problems and opportunities to Communications. Communications provides regular situation reports to Planning and Intelligence to inform the Incident Action Plan.
- Health and Safety (Incident Management Team)
  - Health and Safety works with Communications to ensure that operations are as safe as possible.

Logistics Manager

Role
Supports the response by obtaining, providing and maintaining facilities, services and materials. The Logistics Section ensures that resources are available and tracks them as far as the Operational Area (the Staging Area being a logical divide). When working for the Operations Manager, any resource is tracked by the Operations Section.

Supervises
The staff members within the Logistics Team.

Reports To
The Incident Controller.

Key Objectives

- Protect life
- Protect Company property
- Relieve distress
- Provide support for the most expedient return to normal operations
- Direct the Logistics Section

Responsibilities

- Get to the Emergency Operation Centre as soon as possible
- Obtain briefing from the Incident Controller
- Record decisions, actions and other activities
- Estimate future service and support requirements
- Provide (prepare to provide) supplies, facilities, communications, medical, catering, refuelling and mechanical as required
- Plan the organisation of the Logistics Section
- Appoint, brief and task staff
- Support and supply incident facilities
- Process requests for additional resources
- Help prepare the Incident Action Plan
- Identify possible resources including details such as transport, costs etc.
- Advise Operations of resource availability
- Provide management support

Key Relationships

- Incident Controller
    - The Incident Controller makes requests of Logistics.
    - The Incident Controller supports Logistics by facilitating major requests for resources/release of staff for operations.
    - Logistics attempts to anticipate resource needs based on Incident Controller's stated goals and priorities.
    - Logistics informs the Incident Controller of shortages.
- Operations (Incident Management Team)

  - Operations requests resources from Logistics.
  - Operations relies on Logistics to track resources through non-operational phases (rest, meals, fuelling and maintenance).
  - Logistics attempts to anticipate operational needs.
  - Logistics informs the Operations Manager of necessary stand-down, maintenance and re-supply needs of resources.
- Planning and Intelligence (Incident Management Team)
  - Planning and Intelligence provides predictions of incident development to assist Logistics in anticipating needs.
  - Logistics supplies current resource availability and requirements to Planning and Intelligence to populate the Incident Action Plan.
- Health and Safety (Incident Management Team)
  - Health and Safety works with the Logistics Section to see that resources (especially human) are not injured or damaged because of a lack of rest, food, fuel maintenance and or essential supplies.

Planning and Intelligence Manager

Role

Collects information, analyses it and makes plans based on it. The Planning and Intelligence Manager must have a dual focus on both the current situation (to be able to provide regular status reports) and on the future development of the incident to inform the decisions and planning of the rest of the Incident Management Team.

Key Objectives

- Protect life
- Protect Company property
- Relieve distress
- Provide support for the most expedient return to normal operations
- Direct the Planning and Intelligence Section

Responsibilities

- Get to the Emergency Operation Centre as soon as possible
- Obtain briefing from the Incident Controller
- Record decisions, actions and other activities
- Understand the strategic direction
- Prepare the Incident Action Plan
- Communicate with the Incident Management Team
- Communicate with the Senior Emergency Management Group at the direction of the Incident Controller
- Determine information needs
- Gather, clarify, confirm and analyse information
- Observe deadlines and critical information needs
- Appoint, brief and task staff
- Manage the Planning and Intelligence Section
- Maintain maps and display boards for briefings and situation reporting
- Liaise with technical experts

- Conduct planning meetings
- Plan changeovers and demobilisation
- Provide management support

Key Relationships
- Incident Controller
- Operations (Incident Management Team)
- Logistics (Incident Management Team)
- Health and Safety (Incident Management Team)

Health and Safety Manager

Role
To collect and provide information and specialist advice regarding the safety of the emergency situation as it evolves.

Supervises
The staff members within the Health and Safety Team.

Reports To
The Incident Controller.

Key Objectives
- Protect life
- Protect Company property
- Provide for the welfare of those involved
- Relieve distress

Responsibilities
- Get to the Emergency Operations Centre as soon as possible
- Obtain briefing from the Incident Controller
- Understand the strategic direction
- Liaise with the operations manager to ensure safe point forward, specific controls, etc.
- Identify key hazards and risks relevant to the situation/event
- Provide detailed management plans for the identified risks/hazards for the Incident Action plan
- Contact specialists to provide advice based on the situation
- Prepare and disseminate specific action plans relating to the safety of the incident
- Liaise with the emergency services on advice of the hazards
- Conduct planning meetings to manage hazardous situations
- Appoint, brief and task staff
- Plan change over's and demobilisation
- Advise on the notification process to authorities as required
- Identify likely welfare requirements and initiate action plans accordingly

Key Relationships
- External emergency services

- Internal experts
- Incident Management Team members
- External compliance agencies

Administration Assistant

Role

To provide administrative support for the Incident Management Team and the Emergency Operations Centre. This is the position that the Incident Management Team will look to for all administration, as well as the welfare of the team.

Reports To

The Incident Controller.

Key Objectives

- Manage incoming and outgoing communication
- Manage reception at the Emergency Operation Centre
- Maintain a rolling 24 hour timeline
- Manage the Emergency Operation Centre stores and facility to meet the needs of the Incident Management Team
- General support to the Incident Management Team

Responsibilities

- Receive and issue all communications using the standard message pads
- Pass all incoming communication to Planning and Intelligence (communication may be via landline phone, cell phone, fax, satellite phone or radio)
- Ensure quality of message handling is high
- Make calls on behalf of members of the Incident Management Team.
- Act as receptionist for the Emergency Operation Centre (visitors should not be allowed into the Operations Room unless invited by the Incident Controller - visitors will be briefed in the open briefing area)
- Maintain a rolling 24 hour timeline focused on plotting key deadlines; call scheduling, any bring- up functions, tea breaks or meal breaks
- Give timely reminders in advance of briefings or meetings (other people may become very focused on the detail of their roles; remind them of impending deadlines and follow up on any required information for report preparation)
- Check stock levels and replenish, preferably outside of an emergency situation (maintain cabinets and location stock sheets indicating the minimum that should be present; make a note of expiry dates and replace expired items such as food and batteries as required)
- ensure document templates and stationery stores are maintained
- Type reports as required

Key Relationships

- Incident Management Team members

- Strategic Emergency Management Group

Appendix B - Strategic Emergency Management Group Key Roles

Chair

Role

Leads the Company's strategic response to an emergency through the Strategic Emergency Management Group.

Key Objectives

- Make decisions which require the highest level authority in the Company
- Provide strategic direction for the Incident Controller
- Ensure that communications with the Company employees
- Ensure the financial short term and longer term implications are handled
- Oversee the implementation of the Company's business continuity plan

Responsibilities

- Make timely and considered decisions as required
- Co-opt additional members of the Strategic Emergency Management Group as required
- Make decisions about the State of Company Emergency, Alert Statuses, and Company closure
- Ensure that required information is effectively communicated to the wider Company community (including families of staff and Employees)
- Resolve immediate financial issues created by the emergency event and ensure that necessary resources required by the Incident Management Team are made available
- Implement the business continuity plan as required
- Ensure that appropriate deputies or nominees have been identified in both the Incident Management Team and Strategic Emergency Management Group to cover those who are absent or not available at the time of the Emergency

Key Relationships

- Strategic Emergency Management Group
- Incident Controller and Incident Management Team
- Communications Team
- Wider Company community
- Relevant external parties

Recovery Manager

Role

Facilitates and coordinated the medium and long term recovery activities of the Company following a State of Company Emergency.

Key Objectives

- Ensure that the Company is fully operational again as soon as practicable.
- Keep key stakeholders advised of impact and progress

Responsibilities

- Establish that all measures have been taken to ensure the immediate and ongoing safety, health and welfare needs of those affected have been met (including the Senior Emergency Management Group, Incident Management Team and Communications Team)
- Oversee the restoration of essential services with minimum interruption
- Facilitate and coordinate the Company recovery activities, including the assessment of tasks, setting of priorities, and allocation of resources
- Ensure that existing financial commitments are reviewed and allocations re-targeted to recovery priorities
- Identify areas where existing policies are unlikely to be sufficient or are no longer appropriate to achieve the required recovery level, and where appropriate, create new policies for the recovery phase
- Where possible, continue to meet external obligations
- Establish regular dialogue with key stakeholders to ensure their buy-in and awareness of the intended recovery process
- Regularly report progress to the Director, senior management, and Company staff and Employees

Key Relationships

- Service Divisions and their Directors
- Other Company staff, Employees and parents.
- The wider Company community (outreach facilities)
- Other tertiary providers (particularly those with whom the Company has Memorandums of Understanding)
- Key stakeholders

Appendix C - Pandemic/Epidemic Issues for Specific Company Functions/Areas

The following issues are Company-wide in scope and as such, require a degree of forethought for any one department/division to be able to respond appropriately during a pandemic/epidemic situation. Relevant Company areas are encouraged to take these issues into account in departmental planning for a pandemic/epidemic event.

Functions and areas covered in this appendix:

- Human Resources
- Information Technology Services (ITS)
- International Office
- Proctor's Office
- Property Services
- Employee Health
- Company Union
- Travel

Human Resources

The primary effects of a pandemic are on staffing and Employee levels. Absenteeism may be high due to illness, caring for family members.

During a pandemic/epidemic, Human Resources can only track and record employee absences to determine staff absenteeism rates if staff put sick leave applications through Web Kiosk. As employee absence information will form the basis for decisions by the Incident Management Team around social isolation issues (e.g. postponement or delay of public activities) it is vital sick leave applications are made immediately if staff members knows they won't be coming into work.

The following will apply:

- Initially, if the Company is closed, all employees will continue to be paid. This decision will be reviewed as the duration of the closure is being assessed.
- Employees who are unable to attend work due to illness will be covered by the sick leave provisions in appropriate collective agreements.
- Employees may be required to work from home.
- Maintenance of payroll will be given priority. Where any disbursement is inaccurate, the Company will take corrective steps in the recovery phase. The processing of paper-based timesheets will be either partially or fully suspended.
- Managers and Human Resources staff will work with employees and their union/association representatives to provide cross training/reassignment of employees and/or employee duties to deal with any issues around increased workloads due to temporary loss of staff.
- Employees will be educated on symptoms and will be required to stay home if showing symptoms.

- Employees who are showing symptoms, or who are caring for dependents who are showing symptoms will be required to put a sick leave application through the Web Kiosk as soon as they know they won't be coming into work.
- The Incident Management Team will ensure staff understand the Incident Management Team's need to have access to employee information concerning health issues.
- Financial Services will need to have plans in place to process a Direct Credit file to the bank.
- ITS will need to keep HR systems running and allow remote access to those systems from staff homes via the internet.

Information Technology Services (ITS)

During a pandemic/epidemic, it is likely that ITS systems will become less reliable as they become overloaded with increased volume. If the Ministry of Health mandates social isolation – i.e. directs the closure of companies and public events and encourages the public to stay home – more staff and Employees will need to work remotely and this will result in increased demand on the Company's network and links to the internet.

ITS will inform the Company, via the Incident Management Team about issues surrounding working remotely, and IT alternatives to holding meetings and giving presentations.
The following will apply:

- All ITS delivered training will be cancelled.
- Software for Employees available in Shared location; software for staff can be accessed on-line and managed via Remote Access.

International Office

The International Office is responsible for continuing to provide essential services during a pandemic/epidemic event, including:

- looking after international Employees of the Company, including Employees that might be affected by an infectious disease outbreak in their home country, and
- looking after domestic Employees overseas on exchange at one of offsite location in a country that might be affected by a pandemic.

Property Services

The decision to keep a building open or closed will require input and consultation from the building's main users, Property Services, the Office of Risk, Assurance and Compliance, the Proctor's Office and Health and Safety in coordination with the Incident Management Team. There are two potential reasons for closing a building:

i. the main occupants cannot staff the building and its use is no longer required;

or

ii. there are not enough support staff to ensure a clean, healthy, and safe work environment for the main users.

Thus, the decision making regarding the opening and closure of buildings must be coordinated through the Incident Management Team to assist with the most efficient allocation of staff during a pandemic/epidemic.

The following will apply:

- Services will be maintained as long as possible provided there are enough staff available. Cleaning of toilets and public areas will be a priority. New construction will be minimal.

- Major utility providers will continue to provide service.

- In the event of part or full closure of the Company, only essential services will be maintained (routine maintenance work will not be done).

Employee Health

During a pandemic, primary care services, including vaccinations, will be organised and coordinated by Employee Health staff. The Counselling team at Employee Health will provide psychological services during a pandemic/epidemic for those suffering from emotional trauma or post-traumatic stress.

Travel

A pandemic/epidemic will limit both domestic and international travel and it is likely that travel restrictions will be advised and strongly encouraged. Each department is expected to look after Employees and staff travelling on Company business (e.g. domestically or internationally). When there is a confirmed human outbreak overseas, the Incident Management Team will make decisions about future travel based on the situation. Decisions could include recalling staff or Employees from travel, restricting or limiting travel, and cancelling future travel. In all situations, assistance for international Employees and researchers, and visa management, will be part of the Company-wide response.

Appendix D – ITS Disaster Recovery Plan Recovery Objectives

Following a disaster, Company will recover services using a structured approach. A simple recovery order has been created based upon tiers and sequence numbers.

The Availability Strategy (AS) for an individual service, categorises the planned recovery behaviour of a service in a datacentre failure, and can be used to identify those systems requiring manual recovery intervention versus those that should continue to function with little or no interruption to service.

The Availability Strategies used by company are:

HA (Highly Available): Services designed to survive the loss of a datacentre without interruption from the client's perspective. Clustering or other technologies are deployed that mean services should automatically failover between the datacentres without intervention.

FO (Failover): Services requiring failover require specialist IT action to recover from the loss of a single data centre. Clustering or other technologies are deployed that will synchronise system state and data between both datacentres, however in the event of a disaster, IT specialist actions may need to be taken for the service to resume running from the failover site.

SIP (Single Instance (Protected)): Services that in the event of the loss of a datacentre, rely on the Corporate vSphere stretch cluster's inbuilt HA recovery functionality to resume operations. This system has points of failure that are protected by other mechanisms - typically VMs on the Corporate VMWare Farm. Services using this availability strategy may restart during the DR failover event.

SI (Single Instance): Services that run on a single physical server in one of the datacentres – if that data centre is lost, additional hardware would need to be obtained and commissioned, followed by recovery via the backup system. Service exists in only one datacentre – typically related to a physical piece of hardware due to the heavily virtualised nature of our environment.

DCO (Datacentre Only): Only affects things in the same datacentre – relevant for a partial failure of a site. Only relevant to the datacentre it is deployed in – typical example is DC ToR that is needed for equipment within the same DC.

Recovery Time Objectives (RTO) have been established and are the time within which an IT service must be recovered after a disaster. It is the amount of downtime the business is willing to accept for that service.

In some areas we have expanded on this further to cover two separate scenarios:

RTO Datacentre Failure: The estimated time for a service to be restored in the event of the loss of an entire Data Centre. This time is dependent upon successful recovery of services within all previous tiers – and so is calculated by summing the total time required to recover all preceding tiers.

RTO System Failure: The estimated time for a service to be restored in the event of the loss of just that system.

Recovery Point Objectives (RPO) have been identified and are the point in time to which an IT service and its data must be recovered following a disaster. As such this is also a measure of potential data loss in a worst case scenario.

The following tables list the RTO and RPO of each service.

Tier One Services – Network Infrastructure
The initial focus will be to restore core network services as that is a key requirement for any services.

			RTO	RTO Tier	
/			System	Datacentre	
Seq	System	AS	Failure	Failure	RPO
01 10	Network - Core (Legacy) Network - Core	HA	1 Hr	1:00	N/A
01 20	Network - DNS / DHCP (Legacy)	HA	1 Hr	2:00	Near 0
01 20	Network - DDI (DNS / DHCP / IPAM)	HA	N/A	N/A	Near 0
01 20	Network – Datacentre ToR	DCO	N/A	N/A	N/A
01 20	Network – Datacentre ToR(Legacy)	DCO	N/A	N/A	N/A
01 30	Storage – Block (Corporate)	HA	1 Hr	3:00	Near 0
Tier RTO for Datacentre Failure				**3:00**	

Tier Two Services – Systems Infrastructure

Restoration of several core components essential for lower layers.

			RTO System	RTO Datacentr	
02 10	Central Backup [10] (Base system to begin individual	FO	2 Hr	5:00	24 Hours
02 10	Central Backup [10] (All index data)	FO	15 Hr	*15:00*[11]	24 Hours
02 10	IAM – Active Directory (REGISTRY Domain)	HA	1 Hr	4:00	Near 0
02 10	IAM – Active Directory (EMPLOYEE Domain)	HA	1 Hr	4:00	Near 0
02 10	Network - Load Balancing	HA	1 Hr	4:00	N/A
02 10	Network - Load Balancing (Legacy)	SI	N/A	N/A	N/A
02 20	High Capacity Storage [1] (Supporting Critical / Significant Systems)	FO	1 Hr	6:00	1 Hr
02 20	High Capacity Storage [1] (All other shares)	FO	4 Hr	*9:00*[11]	4 Hr
02 20	Cisco ISE (Identity Services Engine)	FO	N/A	N/A	
02 30	VMWare – Corporate [2]	HA	1 Hr	7:00	Near 0[2]
02 30	VMWare – DMZ	SI	N/A	N/A	N/A
02 30	VMWare – Standalone	SI	N/A	N/A	N/A
Tier RTO for Datacentre Failure				**7:00** **15:00**[11]	

Tier Three Services – Defined Critical Systems

This is the beginning of restoration of service to the first group of Critical Systems.

Tier / Seq	System	AS	RTO System Failure	RTO Datacentre Failure	RPO
03 10	IAM – Active Directory (NET Domain)	HA	1 Hr	8:00	Near 0
03 10	Staff Email	HA	1 Hr	8:00	Near 0
03 10	Employee Email	HA	1 Hr	8:00	Near 0
03 20	RSA Two Factor Authentication	HA	N/A	N/A	Near 0
03 20	Database Services	FO	1 Hr	9:00	Near 0[4]
03 30	Linux Server Management	SIP	1 Hr	10:00	Near 0[4]
Tier RTO for Datacentre Failure				**10:00**	

Tier Four Services - Defined Critical Systems

Continuation of restoration of Critical Systems.

Tier / Seq	System	AS	RTO System Failure	RTO Datacentre Failure	RPO
04 10	Cardax	HA	1 Hr	11:00	Near 0
04 10	Identity Management (IM +SSO) +	HA	1 Hr	11:00	
04 10	Emergency Broadcast System	SIP	N/A	N/A	Near 0 [4]
04 10	Phone System	SIP	N/A	N/A	Near 0 [4, 6]
04 20	Corporate Applications	HA	1 Hr	12:00	Near 0 [5]
04 20	Identity Services	SIP	1 Hr	12:00	Near 0 [4]
04 20	Storage - Block (Employee Desktop)	DCO	N/A	N/A	N/A
04 20	Company Website	SIP	1 Hr	12:00	Near 0 [4, 5]
04 20	Central Logging	FO	N/A	N/A	Near 0 [4]
04 30	Finance	HA	1 Hr	13:00	1 Hr [3]
04 30	HR Payroll	SIP	1 Hr	13:00	Near 0 [4]
04 30	SMS	HA	1 Hr	13:00	Near 0 [5, 7]
04 30	Sophos Antivirus	FO	1 Hr	13:00	Near 0 [4]
04 30	Zoom	FO	1 Hr	13:00	Near 0 [4]
04 40	Business Objects Reporting	HA	1 Hr	14:00	1 Hr [3,5]
04 40	Employee Desktop	HA	1 Hr	14:00	Near 0 [8]
04 40	Employee Printing	SIP	1 Hr	14:00	Near 0 [4]
04 50	High Speed Data Transfer Service	HA	N/A	N/A	
Tier RTO for Datacentre Failure				14:00	

Tier Five Services – Defined Significant Systems

Restoration of service to Significant Systems.

Tier / Seq	System	AS	RTO System Failure	RTO Datacentre Failure	RPO
05 10	OURDrive	HA	N/A	N/A	Near 0 [4]
05 30	Wikis	SIP	N/A	N/A	Near 0 [4]
05 30	HR Recruiting	SIP	1 Hr	15:00	Near 0 [4]
05 30	WSUS	SIP	N/A	N/A	Near 0 [4]
05 40	Blogs	SIP	N/A	N/A	Near 0 [4]
Tier RTO for Datacentre Failure				15:00	

Tier Six Services – All Other Production Systems

Restoration of service to all other servers within the ITS Data centres. This will include a number of internal ITS servers as well as SAAS (Hosted) platforms and IAAS (Housed) servers for departments.

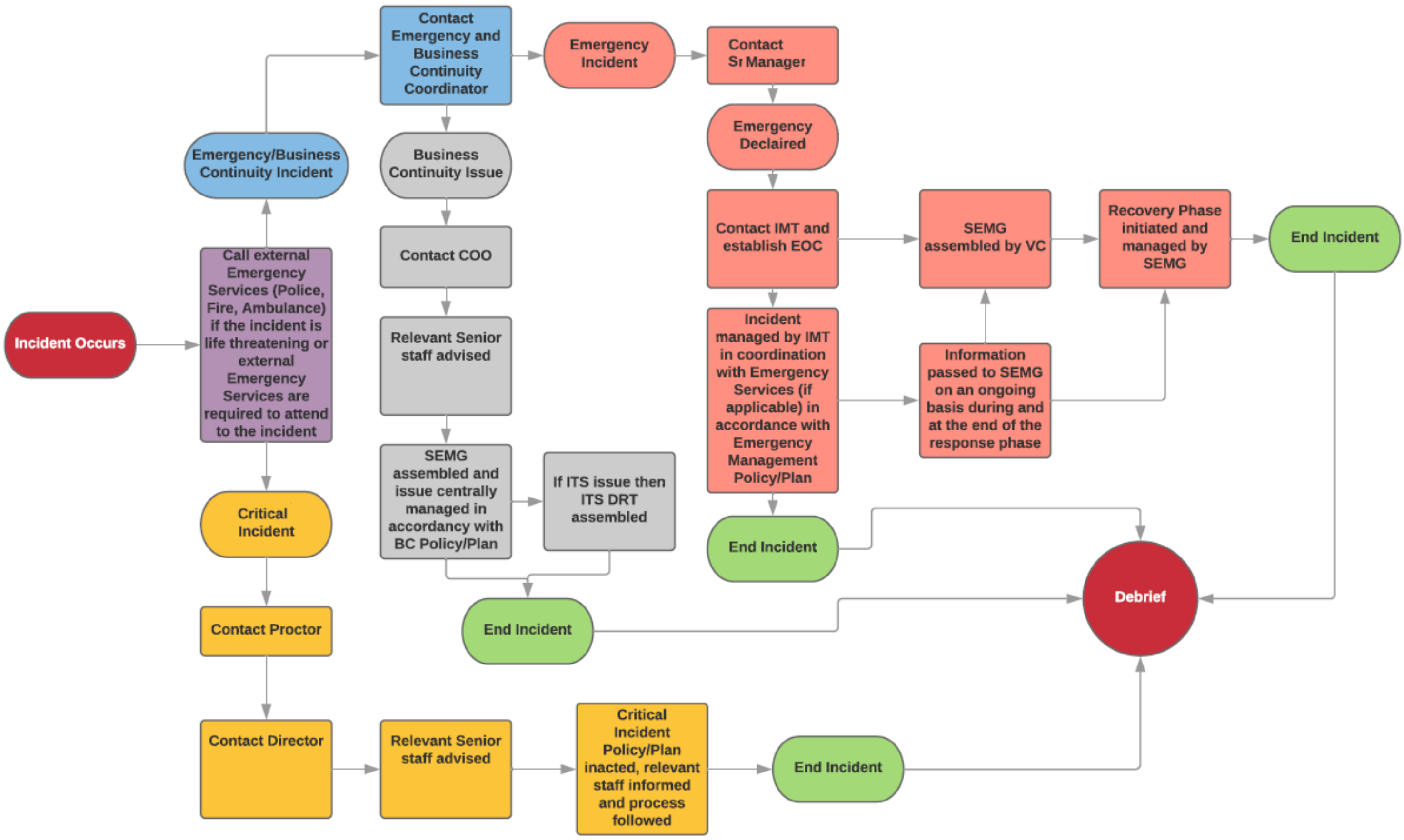
/ Seq	System		RTO System Failure	RTO Tier Datacentre Failure	RPO
	All Other Production Systems				Various [9]

Tier Seven Services – Development / Test / Training

The focus of restoration and verification of systems in the previous tiers is around restoring Production servers however many environments also have Development, Test and Training environments; some of which may be required as part of recovering services – i.e. releasing emergency code updates to mitigate a missing dependency.

Appendix E – Critical Incident/Emergency Response Flowchart

CRITICAL INCIDENT/EMERGENCY RESPONSE FLOWCHART


Incident Occurs
Call external Emergency Services (Police, Fire, Ambulance) if the incident is life threatening or external Emergency Services are required to attend to the incident
Emergency/Business Continuity Incident
Contact Emergency and Business Continuity Coordinator
Emergency Incident
Contact Sr Manager
Emergency Declaired
Contact IMT and establish EOC
SEMG assembled by VC
Recovery Phase initiated and managed by SEMG
End Incident
Incident managed by IMT in coordination with Emergency Services (if applicable) in accordance with Emergency Management Policy/Plan
Information passed to SEMG on an ongoing basis during and at the end of the response phase
End Incident
Business Continuity Issue
Contact COO
Relevant Senior staff advised
SEMG assembled and issue centrally managed in accordancy with BC Policy/Plan
If ITS issue then ITS DRT assembled
End Incident
Debrief
Critical Incident
Contact Proctor
Contact Director
Relevant Senior staff advised
Critical Incident Policy/Plan inacted, relevant staff informed and process followed
End Incident

Review and Revision

The Emergency Management Plan will be reviewed and revised in accordance with the **Emergency Management Policy**.

Recommended: ________________________ Signature

Pakkirisankar Jagannath

Program Manager

Approved: ____________________________ Signature

Anil Sharma

CEO