Working together to build a better future

| P279 | OUTAGE PROCEDURES |
|---|---|

## 1. General Procedure

There are two types of outages: planned and unplanned.

Planned outages can often be scheduled at an optimal time to minimise disruption of usual business activities and can be communicated to relevant staff in advance in order for contingency plans to be prepared.

An unplanned outage is likely to cause some form of interruption to business continuity and can result in financial and reputational loss. The general processes to be followed in responding to an unplanned outage will usually include the following:

- Assignment of responsibility – beginning with an assigned Incident Commander who delegates actions to others.
- Identification of steps to resolve the specific outage (ideally prepared in advance for outages that are able to be anticipated).
- Managed internal communications, ideally utilising a recordable meeting format such as Zoom or Slack meetings.
- Managed external communications as appropriate.
- Managed customer communications as appropriate.
- Structured situational reports to internal stakeholders at appropriate levels of detail and frequency.

## 2. Key Contact Details

| Name | Role | Phone |
|---|---|---|
| ***Internal*** | | |
| Jeremy Mills | CEO | 0481 093 747 |
| Noel Cornwill | COO | 0430 378 051 |
| Sarah Maynard | GM Services & Accommodation | 0414 702 606 |
| Bronni Siggs | GM Business Development & Culture | 0488 757 721 |
| Leigh Goodenough | GM Corporate Services | 0429 806 366 |
| Ryley Johns | GM Quality, Learning & Development | 0400 956 300 |
| Briony Drapala | GM Support Coordination | 0448 123 814 |
| Puneet Chauhan | Assets & Systems Officer | 0449 206 389 |
| Jamie Denyer | Marketing & Communications Officer | 0402 460 499 |
| Jordon Lee | Senior Finance Officer | 0434 581 710 |
| | | |
| ***External*** | | |
| Bruno Dissegna – Comwire IT | IT Support Provider Representative | 0477 016 639 |
| Comwire IT Helpdesk | IT Support Provider | 1300 266 947 |
| Liveware | IT Application Provider – NAV, CIMS | 02 4921 8333 |
| Dave Coleman – SEOWeb Creative | Website Developer | 0423 600 733 |

| | | |
|---|---|---|
| Nigel Gillions – Teleclock | Teleclock Developer | 0409 300 370 |
| Heath Grimmer – Account Manager | Telstra Support | 08 8241 8555 |
| Bhaj – Telecommunications technician | Phone line support | 0438 839 321 |
| SA Power Networks - Emergency | Electricity provider – emergencies | 13 13 66 |
| SA Power Networks - Service | Electricity provider – customer service | 13 12 61 |
| Security Alarm Monitoring Service | Security / Alarm Monitoring service | 1300 365 151 |
| Ian Salvemini - GIASA | Insurance Broker | 0414 490 631 |
| Angela Gregory | Accountant | 0409 513 481 |
| Westpac SME Banking | Bank | 08 9230 2484 |
| NDIS Commission | Regulatory Body | 1800 035 544 |
| SAPOL Emergency | Police – Non-urgent | 131 444 |
| SAPOL Local Station – Hindley St | Police - Callout | 08 8303 0525 |

## 3. Specific Outage Response Plans

### 3.1. Planned Outage

The Assets & Systems Officer or GM Corporate Services will usually take responsibility for managing a planned outage.

A planned outage may be requested for hardware / software maintenance and upgrades, or to cross over services. This will usually be low impact and should involve:

- Identifying a suitable time for the outage (ideally outside of regular business hours).
- Confirming the amount of time required for the outage, and where possible obtaining this in writing.
- Confirming the scope of the outage – which hardware / software / services will be down during this period.
- Communicating the outage to all staff who may be directly affected, in a timely fashion – ideally up to 24 hours before the scheduled outage.
- Communicating the outage to relevant management staff within the organisation
- Setting a calendar reminder for staff and management as relevant
- Providing a last minute reminder and, where feasible, checking in directly with staff regarding the outage immediately before, during and after the scheduled time period.

### 3.2. Unplanned Outage

An unplanned outage may relate to:

- IT hardware (eg computers, server)
- Telecommunications hardware (eg telephone connections)
- Software applications
- Internet connections
- Utility connections (eg electricity connection)
- A combination of the above

Initial assessment is important. An outage can be short term and may become resolved without requiring intervention. It is important to try basic measures such as restarting equipment or applications, checking indicators and meters for confirmation of connections, or asking a support staff member for assistance, before taking further steps to escalate the matter.

If the outage is significant and/or the cause is unknown, the following are essential first steps:

- Identify the Incident Commander (IC) for the outage. As a default this is the CEO, or their delegate. Depending on who is available to respond at the time of the outage, the IC may be the most senior staff member available or the staff member with the greatest technical knowledge of the matter.
- Identify a series of steps to respond logically to the outage. In some cases possible outages may be anticipated. In these cases plans with associated resources and data/information can be prepared ahead of time to support response.

Communication is vitally important during a significant outage:

- Utilise an established medium for internal communication with stakeholders who have a role to play in responding to the outage and to communicating updates to other staff / customers / stakeholders. This may be in the form of face-to-face meetings, Zoom / Slack meetings, or teleconference. It is important for discussion and action points to be recorded and shared with key personnel from these meetings, either via written notes or by recording video / phone conferences.
- For an outage of significant duration or with a particular impact on Customers, business continuity or reputation, internal response meetings should consider and delegate actions for planned communications with Customers and relevant external stakeholders. All communication of this nature should be confirmed by the IC and delegated to specific personnel to carry out.

- Staff can become highly anxious during a significant outage, so it is important to plan and communicate situation reports to staff at appropriate timeframes. The content for these reports should be confirmed by the IC and be carried out by the IC or an appropriate delegate.

In cases where an outage occurs after hours and where decision-making is required, notify the CEO who will delegate responsibility for actions as required. Where there are only simple, unambiguous responses required which can be undertaken by the on-call staff member there is no need to contact the CEO at this time; in this case, management should be notified of the event the following work day.

The after hours call-out listing held by our security monitoring company is as follows:

1. Deb Anderson 0410 055 276
2. Jeremy Mills 0481 093 747
3. Service Delivery A/H 0433 769 157

### 3.2.1. Software Outage

In the case of a software outage, it is essential to consider:

- The core functions of the software
- What information and processes are managed by the application
- What is the timeline before an outage begins to cause problems with service response and business continuity; and how severe are these problems likely to be?

Action plans or checklists for specific software applications include:

<u>CIMS</u>

- Contact Liveware immediately for support.
- Communicate as appropriate with management, the Service Delivery team, the Quality & Engagement Officer and the Assets & Systems Officer.
- Ensure that Customer phone details are kept up to date on Service Delivery after-hours phones in order to maintain connection with Customers.
- Consider strategies for maintaining a separate back-up of rosters, ideally in an editable format that can be merged with CIMS when the application becomes available again. Fortnightly printing of rosters is a base measure.
- Consider strategies for maintaining a back-up of Customer details in the case that NAV is experiencing an outage at the same time (eg during a server or app server outage).

- Consider strategies for maintaining a separate back-up of the incident management system, ideally in an editable format that can be merged with CIMS when the application becomes available again.

NAV

- Contact Liveware immediately for support.
- Communicate as appropriate with management, the Finance team, the HR team and Assets & Systems Officer, and the external accountant.
- Consider strategies for maintaining a back-up of Customer details in the case that CIMS is experiencing an outage at the same time (eg during a server or app server outage).
- Consider strategies for maintaining accessible back-ups of other databases of information contained on NAV. In particular, ensure strategies are in place for an appropriate back-up of HR and financial records.

Teleclock

- Contact Nigel Gillions (Teleclock developer) immediately for support.
- Consider strategies for an alternative method of collecting and storing clock in/out times during an outage which can be easily merged with the system when it becomes available again.
- Establish a communication plan with staff during the outage to maintain data collection processes.

Website / Website Portal

- Contact Dave Coleman (website developer) immediately for support.
- Establish a communication plan with stakeholders utilising the website portal for the duration of the outage.

### 3.2.2. Hardware Outage

Possible hardware outages include:

- A server outage and/or application server outage.
- An outage affecting other network equipment.
- An outage affecting local devices (PCs, laptops, etc).

For initial diagnosis of hardware outages, contact the Assets & Systems Officer or the GM Corporate Services. Any outage that cannot be internally resolved should be referred to Comwire.

| P279 | OUTAGE PROCEDURES |
|---|---|

A significant server outage can result in loss of access to shared drives and key software applications including NAV and CIMS. Where a server outage has affected the application server, contact Liveware in addition to Comwire so that the two support agencies can work together to resolve issues.

Comwire maintains data backups in the case of data loss on server drives. Liveware maintains backups of application settings and modifications for NAV and CIMS.

In responding to a significant hardware outage, the IC should take into account:

- Prioritised follow-up from Comwire / Liveware regarding resolution.
- Determination of the extent of data back-ups available in the case of data loss or corruption.
- Coordination with staff regarding generation and storage of data during the outage.
- Communication with staff and other relevant stakeholders regarding the extent of the outage and the probable timeframe for resolution.

### 3.2.3. Telecommunications Outage

A telecommunications outage may be caused by failure of infrastructure (eg caused by heat, lightning or stormwater) or by a failure of organisational IT equipment (eg network hardware, handsets or headsets). Service cutoff by the provider is another possibility, which should be rare provided that service bills are paid in a timely fashion.

Key support contacts in the case of a telecommunications outage are:

- Heath Grimmer – Account Manager, Telstra: 8241 8555 / heath.grimmer@tbtcsanorth.com.au
- Bhaj – Telecommunications technician: 0438 839 321
- Comwire: 1300 266 947 for support with network hardware and other local hardware issues.

Diagnosis for a phone outage should be sought as soon as possible to determine whether it involves issues outside of the organisation's direct control (and thus will be of indeterminate and possibly lengthy duration).

Continuity of phone service during a long outage should be maintained by switching to use of after hours mobile phones (or by keeping the mobile phones active during business hours as well as after hours, if preferable or more feasible).

### 3.2.4. Utility Outage

The impact of a power outage can be offset by the following measures:

- The server should still be operational due to being located offsite with backup power supply.
- Staff should be able to continue working onsite from laptops for a short time period depending on battery levels.
- Working remotely in locations where power is still available should be arranged where feasible, to facilitate ongoing work during the outage.

Onsite resources such as photocopier and wifi connectors will go down with a power outage. Staff will need to access mobile phone internet and hotspot to their laptops in the short term to maintain connectivity.

SA Power Networks (https://www.sapowernetworks.com.au/outages/) offers information on current outages.

### 3.2.5. Internet Outage

An internet outage may affect the NBN connection to office sites, or may affect mobile networks.

Server connectivity should still be achievable if one type of internet connection is down, provided the other connection type is still accessible (eg mobile hotspotting should be tested if the fibre / NBN connection experiences an outage).

If access is lost to server drives or applications, please follow the instructions outlined above for responding to software / hardware outages.

### 3.3. Cyber-Attacks

Hacking and cyber-attacks can take multiple forms, and new types of threats emerge regularly.

The IT support provider Comwire should be contacted as soon as practicable (1300 266 947) upon becoming aware of hacking or another breach of network security / data security. The advice provided by Comwire must be followed as far as practicable to support diagnosis of the issue and to restrict or mitigate the damage caused.

| P279 | OUTAGE PROCEDURES |
|---|---|

General strategies that can be applied in cases of hacking and cyber-attack are:

- Isolate targeted machines – disconnect network cables and shut down machines where appropriate. In some cases it may be appropriate to turn machines off immediately and in the quickest way possible (which may not be the standard operating system shutdown process).
- Ensure uncompromised data backups – Enhanced Lifestyles maintains an onsite data back-up and is working towards an additional cloud-based back-up service for further security.
- Review logs and commission forensic analysis of the problem where possible, to the extent that is appropriate to the scale of the problem.
- Record and back up any evidence gathered. This may include taking photos of monitor screens before shutting devices down or making changes to address an issue. This obviously needs to be weighed up against the risks involved in certain cases in allowing a problem to persist while evidence is gathered.
- Where it is possible to identify the attacker, report them to the appropriate authorities beginning with SAPOL.
- Repair damage – in consultation with Comwire and with other professional support as required.

Where hacking and cyberattack has affected systems leading to an unplanned outage, refer to the section above for response strategies.

Where applicable, refer to the Data Breach Policy in relation to the requirements for eligible data breach notifications, and to the Data Breach Procedures for broader response processes.

| **Documents related to this policy** | |
|---|---|
| Related documents | Q276 Data Breach Policy<br>P276 Data Breach Response Procedure |