NODE4 PARTNER DISASTER RECOVERY PLAN

INTEGRATED MANAGEMENT SYSTEM

Policy and Procedure

Partner Only

08/08/2019

Key Contact Information – Internal Use Only

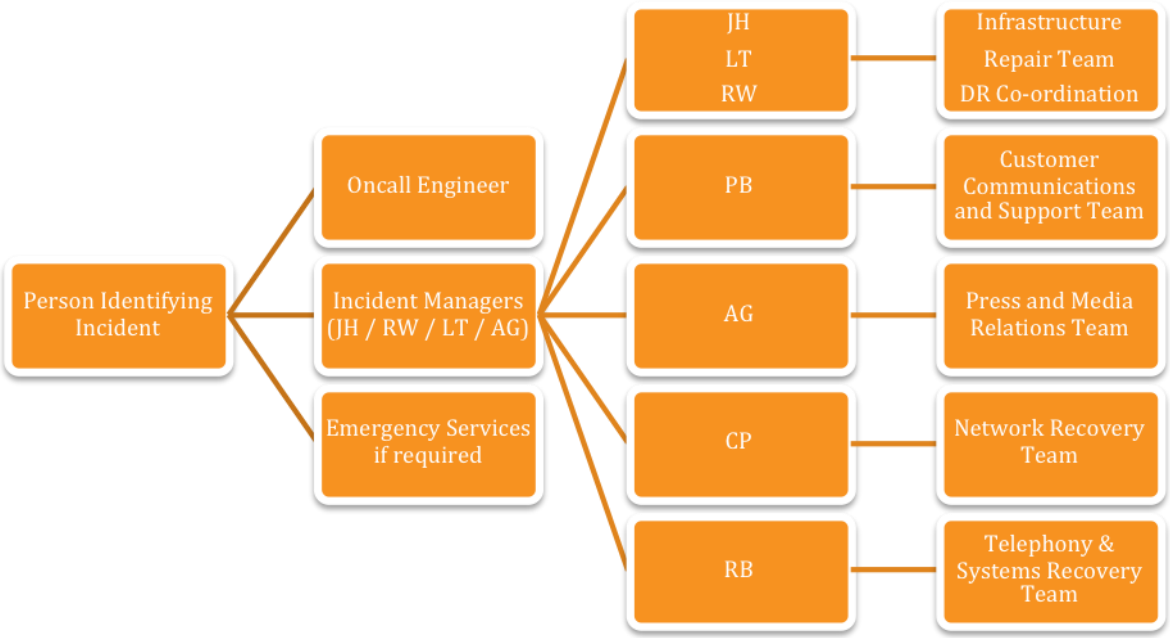
Node4 Contact Information

Staff, contractor and supplier contacts

Communication Summary

Internal Notification Calling Tree

The calling tree below outlines the key teams involved in DR and the team leaders. The Incident Manager will decide which teams need to be involved.



Alternative contacts

In the event of a designated Team leader not being available or contactable, responsibility for that area will be assumed by one of the other team leaders as required, or delegated to a senior member of that team.

Node4 Limited | Millennium Way | Pride Park | Derby | DE24 8HZ | 0845 123 2222 | www.node4.co.uk

DR Plan Scope

For the purpose of this plan, a disaster is defined as loss or damage to all or part of the data centre, infrastructure or offices which would have a high business impact on Node4's ability to provide services to customers.

Elements of DR may be invoked if an event raises risk exposure levels significantly before any actual loss of service. This will ensure that the appropriate levels of management are engaged and that the necessary resources are available to help mitigate risks. (E.g. prior warning of a flood, power interruption etc.).

All Node4 owned sites are included in this scope, namely

- DC1, Pride Park, Derby DE24 8HZ
- DC2, Pride Park, Derby DE24 8HZ
- DC3, Wakefield
- DC4, Northampton

Other sites not under the direct control of Node4 may suffer an outage or disaster that could affect services. These sites have been included in the risk assessments and the risks mitigated where possible by having alternate locations (e.g. dual POPs for internet breakout, multi-homed internet transit and diverse fibre connections).

Power, HVAC, Fire Suppression, Network, Server and Security Infrastructures at all sites is included in the scope

Assets Included

This plan is primarily concerned with restoring the operation of core Node4 services and does not include individual DR plans for customers and their equipment (collocated servers, WAN links, etc.). Any customer DR plans that are the full or partial responsibility of Node4 will be documented separately. Due to the nature of services supplied, restoration of Node4 systems on the same site will also cover customer equipment.

Part of the management of a DR scenario involves liaison with customers and controlling access of visitors to site during an emergency situation.

Trigger Events

Events at any Node4 site that would trigger one or more elements of DR or business continuity:

- Total loss of connectivity to one site
- Fire or flood at any site
- FM200 or IG55 Gas suppression discharge
- Loss of building in other circumstances
- Loss of UPS backed power
- Loss or extended period of severely reduced cooling capacity
- Extended loss of mains power (>24hours)

Incident Management Responsibilities

Incident Managers have been appointed to contain the situation in which the BC / DR Plans are to be deployed. Several incident Managers have been identified to ensure supporting availability in the event that a singular individual cannot be contacted. Their remit is to minimize the impact on service, establish communications with other key personnel and to minimise the time in which normal operations can be resumed.

In addition, 2 of the Incident Managers' contact information are recorded by the BT Redcare Contact Centre and the Derbyshire Constabulary (AG and JH).

In the event of alarm activation outside of normal business hours, these are the two individuals who would be the first to be notified. If a situation arose where neither appointed Incident Managers were able to attend the facility, then responsibility would be passed to the individual who appears in order of seniority on the corporate hierarchal chart.

The Incident Manager will:

- Assess the scope of the disaster and root cause where possible
- Establish a line of communication to all DR Team Managers
- Ensure emergency services are alerted where necessary and have complete access to the facility
- Inform stakeholders and customers of the incident and provide regular updates of the situation (via the DR Team
- Co-ordinate all staff activities relating to the incident
- Informing Node4's insurance company of the incident
- Control access to the facility for customers

Incident Management – Customer PCI Breach

When Node 4 receives a **breach notification**, we are **required** by the **card brands** to investigate and to assist the merchant in containing the **breach** as soon as possible. Failure to do so can result in non-compliance fines levied on the merchant.

It is unlikely unless there is a breach in physical security that we would initiate the first response, but we may be consulted by one of our customers if they have suffered a payment card data breach on one of the systems we are hosting.

As a Service provider, we would always advise our customers to contact their acquirer directly, who will, in turn, inform the payment card brands.

The Data Controller (the customer) should make the ICO aware within the first 72 hours of a payment card breach. Node4's DPO must be contacted in the event of any payment card data breach.

The Data Controller (the customer) should consider contacting Action Fraud to report the crime as soon as possible.

Payment Card Brand details supplied below:

American Express

Website: http://www.americanexpress.com/datasecurity

Email: AmericanExpressCompliance@trustwave.com

Discover

Website: https://www.discovernetwork.com/en-us/

For questions about the DISC program:

https://www.discovernetwork.com/en-us/business-resources/fraud-security/pci-rules-regulations/

Email: DISCCompliance@discover.com

JCB

Website: http://www.global.jcb/en/products/security/data-security-program/

Email: riskmanagement@jcbati.com

MasterCard

Website: http://www.mastercard.com/sdp

Email: sdp@mastercard.com

Visa

Visa Europe

Website: http://www.visaeurope.com/ais

Email: datasecuritystandards@visa.com - for member and merchant requirements

Email: pcidsseurope@visa.com - for service provider requirements

Differences between Disaster Recovery and Business Continuity

Business continuity encompasses all the necessary processes and procedures required to minimise interruption to the normal operation of the business. Disaster Recovery refers more specifically to the steps required to restore normal business functions following an incident.

DR Team Responsibilities

The DR Teams have specific areas of responsibility in a DR scenario to handle communications, system recovery etc. Not all teams will be needed for all scenarios. The appropriate DR teams will be contacted by the Incident Manager as soon as possible following an incident.

Each individual team manager is responsible for mobilising as many team members as is necessary/possible to deal with the situation. Team members may work remotely from home or from another Node4 site during the incident depending on the situation. Some staff may be required onsite to aid recovery.

Infrastructure Team

- Co-ordination of repairs to physical infrastructure (power, cooling, fire suppression, building fabric)
- Co-ordination of temporary infrastructure (e.g. temporary generator sets, fuel supplies etc.)
- Liaison with emergency services
- Control of access to building for staff and customers
- Maintenance of a sufficient standard of physical security

Considerations

Staff and Customer Safety are the primary concerns if the physical infrastructure of the building has been compromised

Customer Communications Team

- Fielding of customer enquiries by telephone or email
- Updating of websites, tickets, emails, SMS and other communication mechanisms
- Handling/prioritisation of remote hands requests

Considerations

Where possible, technical staff should be left to restore services as quickly as possible without dealing directly with customer issues.

Customers should be directed to a central information source (usually n4status.com) to obtain updates from a consistent, reliable source.

Communications team members must ensure that they give a consistent view of events and avoid speculation or unauthorised comments.

Customer Communication Channels

Node4 have several methods of communicating directly with customers. In a DR scenario, one or more of these channels may be temporarily unavailable, and alternatives should be used. The preferred line of communication is via www.n4status.com

System	Primary Hosting Location	Backup / Alternate Location	Comments
Telephone System	Derby	Other Node4 DC	0845 123 2222 and 0845 123 2229 can be redirected by KCOM
Email	Derby	Other Node4 DC	
Ticket System	Derby	Other Node4 DC	
http://N4status.com	IOVPS (London)	Node4 DC (any)	Hosted outside Node4 Network. Can be updated over the internet (3G if necessary). Preferred communications route.

Press and Media Relations Team

- Issuing statements to press/dealing with enquiries/interviews
- Vetting of statements posted on status sites etc.

Network Recovery Team

- Re-establish connectivity and deal with re-routing of traffic
- Liaison with network providers on faults

Systems Recovery Team

- Recovery of internal Node4 systems (email, CRM, SharePoint, Billing Systems etc.) and restoration of data from backups

Telephony Recovery Team

- Re-establish telephony services and liaise with Telco providers on faults

Assumptions

When developing the Disaster Recovery Plan, the following assumptions have been made

- The plan has procedural effectiveness 24 hours a day 365 days a year
- That the deployment of the plan may be required outside of normal business hours
- That the Integrity of the service has been compromised to such an extent that Node4 are unable to meet their contractual obligations
- Normal redundancy/resilience precautions have failed to maintain services (except in the event of a prolonged power outage requiring fuel top-ups)
- Two Incident Managers, holding senior roles within the company will manage the incident
- DR Teams will manage particular communication and technical roles.
- All further staff will have knowledge of the location of the Disaster Recovery Plan and the back-up copy to deputise or manage in the event of the two appointed Incident Managers being unable to co-ordinate activities through absence, injury or death
- Backups of the application software and data are intact and available
- Service and maintenance agreements with hardware and software suppliers are up to date, and both active and passive incident containment machinery are operative
- The incident only affects one physical location (Derby, Northampton or Wakefield)

Node4 Limited | Millennium Way | Pride Park | Derby | DE24 8HZ | 0845 123 2222 | www.node4.co.uk

Risk Analysis

A number of risk assessments are performed as part of our ISO27001 and our quality management systems. These detail risks that may include incidents that would lead to a full or partial invocation of the DR plan, and other more minor risks that may only affect some elements of service. This DR plan is part of the ISO27001 and quality management systems. Risk Assessments are stored in SharePoint.

To reduce the probability of a malicious attack upon Node4's Data Centres and to limit the impact on the operational capabilities of the organization through negligence or an act of god the following active precautions have been taken.

- Our Network topology and diverse data centres will allow re-routing of network traffic in the event of a site loss
- Core network equipment and servers are distributed/replicated between sites
- Network connectivity equipment is situated at TeleHouse, and Global Switch, London and TeleCity, Manchester and are served by physically diverse fibre connections
- Node4's buildings are protected by a perimeter security fence and other security measures
- The premises are protected by numerous CCTV cameras with continuous digital recording
- The buildings are manned 24/7 by staff or security. Security firms have adequate backup personnel available
- Entry to the buildings and datacentres is controlled through electronic swipe cards
- The buildings are protected by a fire alarm
- The data centres are protected by a self-contained gas suppression system containing FM200 gas
- The data centres are protected by a redundant uninterruptible power supply unit (UPS) and a N+1 diesel generator bank
- Backup hardware is tested by the Technical Manager on a monthly basis.
- The network infrastructure (both physical and logical) has sufficient protection from attack
- The buildings have been visited and assessed by the local Fire Officer

Temporary Co-location and Office Facilities

Wakefield and Northampton Data Centres have sufficient free rack space to accommodate Node4 systems and hardware from Derby. Northampton and Wakefield have enough office space to house the majority of staff on a long term basis if required. A summary of the capacity of each site is at the end of this document. General Internet transit is available from all 3 sites, via diverse POPs.

In addition to DC3 and DC4, Node4's 2 data centres in Derby (DC1 and DC2) have separate infrastructures in terms of

- Power supply and backup UPS / Generators
- FM200 Fire Suppression
- Cooling / CRAC Units

Internet connectivity for DC1 relies on DC2. Internet connectivity at other sites is independent (part of MPLS)

Key network components are distributed between the data centres, where possible, providing extra resilience in Node4's core infrastructure. Core network equipment is split between sites and servers are virtualised and distributed. Full High Availability (HA) is being implemented for Node4 systems. Backups are made across the WAN to each alternative site.

Our 3rd and 4th data centres (DC3 – Wakefield, DC4 - Northampton) are in geographically diverse locations. They are linked to Derby via redundant, diverse fibre connections, so in the event of the loss of any one site or fibre link, network traffic can be rerouted. Core services will be distributed as much as possible between sites and our MPLS network, and multiple POPs will allow routing to be reconfigured in case of an emergency.

DR facilities spread between both data centres will be offered for customer equipment as well as Node4 infrastructure if required.

Data Backup Process

All core network device configurations, VM images, databases and other business data are backed up on a regular basis. This information is transferred offsite to ensure physical diversity of data. The frequency of backups and retention depends on the nature of the information. This data includes hardware information, network documentation and network diagrams along with all configuration scripts for network devices appertaining to both customer networks (where appropriate) and to Node4's core network.

These backups are verified as part of the daily checks performed by the tech support engineers.

Backup tapes, where used, are stored in a fire-safe

Core network servers in both data centres are imaged regularly, and the snapshots are backed up as part of this process.

Customer data may also be backed up and stored offsite as part of a full or partially managed DR Service.

Information Security Requirements of DR / BC

Implementation of any elements of the DR/BC plan must not compromise existing information security controls by placing information or access to information in a less secure environment.

Section A17.1 of ISO27001:2013 covers the necessary controls for these requirements.

The DR/BC plan in this document does not involve the use of 3rd party facilities or infrastructure to host people, systems or corporate / customer information for the duration of an incident.

Each Node4 facility that could be used during DR (e.g. to act as a temporary head office or NOC) is subject to the same set of IS policies and procedures.

Each Node4 facility that could be used during DR is connected to the existing network and access is controlled by the same physical and logical controls.

Remote working is covered by the existing teleworking policy and, although more people may work remotely during an incident, the actual risk level would not be increased.

Any physical equipment that would need to be transported between sites as part of a DR/BC incident must be transferred in line with media transfer policies. This includes the use of secure couriers, transfer with authorised Node4 employees or use of trusted 3rd parties such as Technimove.

If the nature of the incident increases IS risk for the duration of the incident (e.g. by reducing redundancy levels of infrastructure, HA of systems or offsite backups), appropriate mitigation steps or risk acceptance should be implemented.

Stages of Business Continuity and Disaster Recovery

At all stages of the DR process, people should follow the advice of the expert in each affected area (emergency services, contractor engineers etc.) and not take unnecessary risks to attempt to restore service or save a property or other assets.

1: Notification / Activation Stage

This stage includes those actions required by the Incident Manager to assess the situation and launch the Disaster Recovery Plan (or parts of it).

On arrival at the facility, the Incident Manager will assess the scope of the disaster and whether recovery is possible from the existing location or whether it is necessary to relocate services to another location, through a visual assessment of the situation.

Consideration will be given to the impact the situation has on the effectiveness to maintain the continuity of the service. This impact assessment will be based upon:

- Advice from Emergency Services or Government Organisations where given
- The structural integrity of the building
- If applicable, the area of the building that is affected and whether safe access is obtainable
- Whether mains power exists
- UPS and generator back up in operation or bypass/standby
- Telephone connectivity
- Internet connectivity
- Air conditioning function and capacity
- Any additional risks that have arisen as a result of the incident
- Whether further interruptions to service are likely (and if it is better to delay restoration of service to avoid intermittent faults)

2: Recovery Stage

The Incident Manager will then delegate responsibility to the team of DR Managers to assess subsystem damage in more detail and begin to restore services from the affected facility or manage relocation to the alternative geographical DC locations.

The recovery stage may involve the purchasing of equipment to restore service. This should go through preferred suppliers and the normal purchasing process where possible. Insurance or warranty replacements should be used wherever these are available. Comms-care may not cover physical damage, only failure of components.

When restoring services, it is important that supporting billing systems are in place first so that financial losses are not incurred.

During the recovery stage, certain elements of the operation may be compromised, and risks must be reassessed on a rolling basis. For example, physical security perimeters and CCTV may be damaged, requiring more security staff to be assigned to a site overnight.

Communications

Depending on the nature of the incident, normal communication routes may be disrupted. One of the priorities of the recovery stage is to re-establish both internal and external communications as quickly as possible. This will be the responsibility of the Communications Team but may involve the telephony, networks and systems, recovery teams.

The internal calling tree at the top of this document should be used to contact the relative staff members who will assist with the DR process.

Staff members not directly involved in the DR process should be contacted and informed of the situation and given direction.

3: Reconstruction Stage

The purpose of the Reconstruction Stage is to return the operation to that state prior to the incident occurring

Once the Incident Manager has declared that normal service has been restored, he will:

- Liaise with the insurance company to ensure successful handling of the claim
- Ensure that all fire control devices and equipment are operationally ready
- Ensure that all necessary security arrangements are made to maintain the facilities integrity
- Inform all stakeholders that normal operations are resumed

Scenarios – Internal Use Only

Scenarios for power, cooling, connectivity, voice and site loss with key considerations and contingency plans