

Internal and Confidential

Netradyne Disaster Recovery Procedure

v3.3

Table of Contents

[Document Control 2](#_Toc668952151)

[3 Roles and Responsibilities 3](#_Toc2027255366)

[1 Procedure 4](#_Toc898798172)

[1.1 Roles and Responsibilities for Disaster Recovery (DR) process 4](#_Toc410984458)

[1.2 Process Flow 4](#_Toc1053386100)

[1.3 ENTRY CRITERIA 5](#_Toc2022196160)

[1.4 Inputs 5](#_Toc1467161442)

[1.5 Activity Performed 5](#_Toc956866111)

[1.5.1 Assess Disaster Situation 5](#_Toc858772028)

[1.5.2 Ensure Employee Safety 5](#_Toc1561845155)

[1.5.3 Communicate to Stakeholders 6](#_Toc945324875)

[1.5.4 Recover Essential IT and Infrastructure Services 6](#_Toc630529954)

[1.5.5 Return to Normal Operation 6](#_Toc345420527)

[1.5.6 Analyse Disaster Recovery Effectiveness 6](#_Toc767755155)

[1.6 Outputs 6](#_Toc45539877)

[1.7 Exit Criterion 7](#_Toc473524699)

[1.8 Measurement and Analysis 7](#_Toc1999750197)

[1.9 Standard Compliance 7](#_Toc1728029211)

[1.10 Recovery Time Objective 7](#_Toc1161809772)

[1.11 Recovery Point Objective 7](#_Toc1650300359)

[1.12 POC in case of Disaster for Infra 8](#_Toc2057234680)

[2 Conduct 8](#_Toc1591352646)

[3 Exception 8](#_Toc1327905630)

[4 Terms/Acronyms 8](#_Toc142093001)

[5 References 9](#_Toc1214000379)

[5.1 Templates 9](#_Toc2014121016)

[5.2 Policies 9](#_Toc1050134033)

[5.3 Process/Procedures 9](#_Toc943401475)

[5.4 Standards 9](#_Toc1077275839)

[5.5 Miscellaneous 9](#_Toc941743658)

[6 Appendix A: Document RACI Matrix 9](#_Toc149375196)

### Document Control

|  |  |
| --- | --- |
| **Document ID** | NDDR2020002 |
| **Document Name** | Netradyne Disaster Recovery Procedure |
| **Document Status** | Released |
| **Document Released Date** | 29-Nov-2020 |
| **Document Author** | InfoSec |
| **Document Content Contributors** | Sudhansu Kumar, Hemchand T., Rajeev Ghosh |
| **Document Signatory** | CISO |
| **Document Owner** | InfoSec |
| **Document Version** | v3.3 |
| **Information Classification** | Internal |

**Document Edit History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Additions/Modifications** | **Prepared/Revised By** |
| v1.0 | 30-NOV-2020 | Original issue. | Vivian Preetham |
| v2.0 | 22-MAR-2021 | Measurement and Analysis | Vivian Preetham |
| v3.0 | 20-JUN-2022 | Annual Review with no changes | Kavitha Shetty |
| v3.1 | 26-APR-2023 | Annual Review with changes in recovery of essential Infra system | Sudhansu Kumar |
| v3.2 | 09-Feb-2024 | Refined to include more controls on data privacy/Data Protection | Hemchand |
| V3.3 | 03-Feb-2025 | Added the RTO, RPO and the POC details | Hemchand |

**Document Review/Approval**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Signatory Name** | **Organization/Signatory Title** | **Comments** |
| 29-NOV-2020 |  | CISO |  |
| 21-MAR-2021 |  | CISO |  |
| 18-JUN-2022 | Saravanan Sankaran | Senior Director InfoSec & IT |  |
| 26-APR-2023 | Saravanan Sankaran | Senior Director InfoSec & IT |  |
| 12-Feb-2024 | Saravanan Sankaran | Senior Director InfoSec & IT |  |
| 05-Feb-2025 | Saravanan Sankaran | Senior Director InfoSec & IT |  |

**Distribution of Final Document**

|  |  |
| --- | --- |
| **Name** | **Organization/Title** |
| All Organization | Netradyne |
|  |  |
|  |  |

**1 Purpose**  
  
Ensure organization is prepared to face disasters, ERT team will be ready and notified during a  
  
disaster. All internal and external stakeholders shall comply with the process in the event of disaster.  
  
**2 Scope**  
  
Scope is lim ited to IT and Infrastructure Services at Netradyne, test plans for infrastructure systems  
  
are scoped and the problems identified are documented and have an associated remediation action.  
  
Testing is perform ed on an annual basis of the DR plan

# 3 Roles and Responsibilities

Roles and responsibilities specific to this document are included below:

|  |  |
| --- | --- |
| **Role** | **Responsibilities** |
| Owner | * Team or SME responsible for the process area needs to ensure this document is up to date and compliant with governing requirements. * Is the point of contact for the document. * Responsible for initiating and managing document review and the approval process from start to finish including gathering or delegating the collection of content including diagrams, formatting etc. as well as identifying stakeholders to participate in the peer review process. |
| Reviewers/Stakeholders | Representations from teams that can affect or be affected by the document under review (e.g., Operation, Security, Compliance, Quality) |
| Approvers | The Person(s) of authority to validate the document and sign-off on the latest version. Such Person include Document owner, Functional Team Lead, Security Lead, Product Delivery Lead. |
| Document Release | Document Owner/team to work with repository administrator to make release version available. |

# Procedure

## Roles and Responsibilities for Disaster Recovery (DR) process

The Netradyne system disaster recovery plan is implemented and maintained. Recovery Time Objectives (RTOS) and Recovery Point Objectives (RPOS) are established and monitored based on client requirements pursuant to compliance with the DR/BCP Plan.

| **Role** | **Responsibilities** |
| --- | --- |
| CISO (**Chief Information Security Officer)** | * + Assess disaster situation and execute necessary action.   + Coordinate with other stakeholders   + Communicate invocation of Disaster Recovery Process to Emergency Response Team |
| ERT (***Emergency Response Team)*** | * + Ensure safety of people |

## Process Flow

Diagram

Description automatically generated

## ENTRY CRITERIA

1. Natural Disaster

2. Technical failure

3. Pandemic

## Inputs

| **#** | **Product Name** |
| --- | --- |
|  | IDMS  Driveri |

## Activity Performed

### Assess Disaster Situation

| **Activities** | **Resp.** | **Related Documents / Processes / Notes** |
| --- | --- | --- |
| Assess Disaster Situation | CISO |  |
| Evaluate whether to invoke Disaster Recovery Process | CISO |  |
| Invoke Disaster Recovery Process, if needed | CISO |  |
| Communicate invocation of Disaster Recovery Process to Emergency Response Team | CISO | Business Continuity Plan |

### Ensure Employee Safety

| **Activities** | **Resp.** | **Related Documents / Processes / Notes** |
| --- | --- | --- |
| Evacuate Buildings | ERT | Fire Policy - HR |
| Ensure Employee Safety | ERT | Fire Policy - HR |
| Provide First Aid | ERT | First Aid Guidelines - HR |

### Communicate to Stakeholders

| **Activities** | **Resp.** | **Related Documents / Processes / Notes** |
| --- | --- | --- |
| Inform employee relatives about Disaster | ERT | To be done by HR |
| Inform Clients about Disaster | ERT | To be done by CSM |
| Alternative modes of operations | ERT | WFH |

### Recover Essential IT and Infrastructure Services

| **Activities** | **Resp.** | **Related Documents / Processes / Notes** |
| --- | --- | --- |
| Inform Vendors for Support, if required | IT |  |
| Restore essential Servers and Systems | IT/Infra | Snapshot Backups, Bucket Versioning, RDS backup for Infra related important artifacts |
| Restore Essential Networks | IT |  |

### Return to Normal Operation

| **Activities** | **Resp.** | **Related Documents / Processes / Notes** |
| --- | --- | --- |
| Assess if the operations have returned to normalcy | CISO |  |
| Inform employees about Normal Operations | ERT | To be done by HR |
| Inform Clients about Normal Operations | ERT | To be done by CSM |

### Analyse Disaster Recovery Effectiveness

| **Activities** | **Resp.** | **Related Documents / Processes / Notes** |
| --- | --- | --- |
| Analyse Disaster Recovery Effectiveness | CISO |  |
| Identify improvements in Disaster Recovery Process | ISMS Forum | ISMS yearly audit will take care of this. |

## Outputs

| **#** | **Description / Work Product Name** | **#** | **Description / Work Product Name** |
| --- | --- | --- | --- |
| 1. | IT and Facilities recovered | 2. | Infrastructure recovered |
| 3. | Process Change Tracker (ISMS Forum) | 4. | Executed DRP |

## Exit Criterion

Normalcy Restored

## Measurement and Analysis

| **#** | **Metric** | **Definition/ Formulae** | **Data to be captured** | **Source** | **Owner** | **Frequency** |
| --- | --- | --- | --- | --- | --- | --- |
|  | 18 months  March 2020 – September 2021 | Due to Pandemic Employees were asked to WFH for a period of 18 months, this was a decision from the higher Management | * IT and Facilities recovered. * Infrastructure recovered. * Process Change Tracker (ISMS Forum) * Executed DRP | CISO/MR | CISO/MR | NA |

## Standard Compliance

| **Standard / Model** | **Clause No & Name** | **Control description** |
| --- | --- | --- |
| ISO 27001 | * A.14 | * Business Continuity Management |

Recovery Time Objective

RTO is the goal that an organisation sets for the maximum length of time it should take to restore normal operations following an outage or data loss.

  We have different kind of disaster scenarios:-

If a minor outage is from the application, or infra, or db side we can handle and fix it in **4 hours**.

In case there is a major outage, we should be able to bring back all services in **24 hours**. We can define our RTO as 24 hours.

If a catastrophic outage is from AWS — like AWS services (S3, EC2, etc.) are down or the entire region is down — we have to wait for the fix from AWS side.

Recovery Point Objective

RPO is the goal for the maximum amount of data the organisation can tolerate losing.

We have a backup for the PostgreSQL DBs every 30 mins. So, we can set our RPO as 1 hour.

For our data stored in S3, we rely upon the durability and availability guarantees provided by AWS — 99.999999999% durability and 99.99% availability of objects over a given year.

POC in case of Disaster for Infra

DevOps POC:

* Alok Mohan [alok.mohan@netradyne.com](mailto:alok.mohan@netradyne.com)
* Soham Chatterjee [soham.chatterjee@netradyne.com](mailto:soham.chatterjee@netradyne.com)

DB POC:

* Boopathi Lakshmanan [boopathi.lakshmanan@netradyne.com](mailto:boopathi.lakshmanan@netradyne.com)
* Gowthaman Sivasankaran [gowthaman.sivasankaran@netradyne.com](mailto:gowthaman.sivasankaran@netradyne.com)
* Raghunath Dhandapani [raghunath.dhandapani@netradyne.com](mailto:raghunath.dhandapani@netradyne.com)

2nd level POC:

* Sudharsan Sivasankaran [sudharsan.sivasankaran@netradyne.com](mailto:sudharsan.sivasankaran@netradyne.com)
* Rakesh Pelluri [rakesh.pelluri@netradyne.com](mailto:rakesh.pelluri@netradyne.com)

# Conduct

Compliance Checks to this process to be performed through various methods, including but not limited to reports, internal/external audits, Awareness training/assessments and feedback to the process owner. Non-compliance will be escalated to the Netradyne leadership team.

# Exception

Exception to this procedure must be approved through the Netradyne Exception Process.

# Terms/Acronyms

|  |  |
| --- | --- |
| **Term/Acronym** | **Definition** |
| DRP | Disaster Recovery Plan |
| Infosec | Information Security |
| ERT | Emergency Response Team |
| BCP | Business Continuity Planning |
| HIPAA | Health Insurance Portability and Accountability Act |
| GDPR | General Data Protection Regulation |
| ePHI | Electronic Protected Health Information |

# References

## Templates

<List of (or Links to) associated templates>

## Policies

<List of (or Links to) associated corporate level policies>

## Process/Procedures

[NetradyneSecurityIncidentResponsePlan\_v1.2.pdf](https://netorg726775.sharepoint.com/:b:/r/sites/NETRADYNEDOCUMENTMANAGEMENTPORTAL/Shared%20Documents/General/NetradyneSecurityIncidentResponsePlan_v1.2.pdf?csf=1&web=1&e=3uMG3b)

[Disaster Recovery ProcessV3.0.docx](https://netorg726775.sharepoint.com/:w:/r/sites/InfoSecDocumentGovernanceRepository/Shared%20Documents/General/BCP_DR2023/Disaster%20Recovery%20ProcessV3.0.docx?d=w44bffbcb50b04c588a6a1e637bc37bcb&csf=1&web=1&e=2IrzF3)

## Standards

<List of (or Links to) related Netradyne Standards>

## Miscellaneous

<List of (or Links to) any relevant documentation not covered in the list above>

# Appendix A: Document RACI Matrix

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Role/Activity | Document Owner/Functional Area Lead | Document Contributor | ND Leadership | Functional Area Team | InfoSec | All ND Member(s) |
| Ensure document is kept current | A | R | I, C | R, C | C | I |
| Ensure stakeholders are kept informed | A | R | - | R | C | - |
| Ensure document contains all relevant information | A | R | I, C | R, C | C | I |
| Ensure document adheres to document governance policy | A, R | R | I | R, C | R, C | I |
| Provide SME advice | I, R | A, R | I | R, C | I, C | I |
| Gathering and adding document contents | I | A, R | I, C | R, C | C | I |
| Document Approval | A | R | I, R | I | I, R | I |

|  |  |
| --- | --- |
| Key |  |
| R | Responsible |
| A | Accountable |
| C | Consulted |
| I | Informed |