Be Rota Limited
Disaster Recovery Policy
Appendix 1

Introduction

This policy provides a framework for the ongoing process of planning, developing, and implementing disaster recovery management for technical services at Rota. A disaster is a serious incident that cannot be managed within the scope of Rota's normal working operations.

Disaster Recovery Incident Operations Include:

a) All activities and steps necessary to restore systems services that are affected by a disaster.
b) All activities concerned with management and user communications related to the disaster.
c) All activities concerned with the mitigation of the impact of an ongoing disaster incident.
d) All activities concerned with the follow-up to an incident.

Disaster Recovery Management

Disaster recovery management is the process of planning and preparation to:

- Identify critical and secondary systems based on risk assessment.
- Establish baseline recovery time capabilities and objectives.
- Maintain and test DR capabilities on an ongoing basis.
- Identify gaps between current and required capabilities for system recovery.

Disaster Recovery Policy Objectives
Disaster Recovery Operations Management

This policy is implemented to minimise the impact of significant incidents on Rota services and recover from the unavailability of systems to an acceptable level through a combination of responsive and recovery controls. To achieve this, the following three objectives are set out:

- Establish operational control of the disaster
- Communicate with relevant parties impacted by the disaster
- Activate a specific recovery plan in relation to the disaster

The disaster recovery plan is invoked when

- A member of the IT Services management team requests the commencement of DR operations.
- If a critical service sustains a P1 service outage which has lasted 24 hours or is determined as likely to do so.

Disaster Recovery Management Planning

To complement this policy, disaster recovery management planning shall conduct risk assessments and ensure scenarios, procedures and plans are developed and implemented for critical business systems to ensure timely resumption of essential services. These plans shall be made available in a convenient form for use by DR Teams and shall be reproduced for distribution to all managers periodically as updated to retain for use. Where critical services are outsourced, IT Services shall ensure that suppliers agree to have similar suitable plans and contingencies in place to meet the criteria for critical systems.

Disaster Recovery Planning Policy

It is neither economical nor practical to maintain fully redundant hardware in preparation for all potential disasters. Rota has implemented cross data centre resilience, where either data centre has the capability to provide adequate operating services to Rota in case of the loss of a single data centre. Disaster recovery is incorporated into the architecture of new systems that are deemed critical by the business. The recovery of a service is governed by the stated, agreed Recovery Time Objective (RTO) for each service, and the level of criticality of each system (here referred to as Tier). A service is a collection of systems and devices that collectively support a business process. The recoverability of a service is governed by the capabilities of the underlying systems in terms of resilience and redundancy, and the time for recovery of the systems if recovery is required.

Within Rota, the following levels of disaster recovery capability apply:

Tier	Applicability	Recovery Objective
1	A Tier 1 system is any customer- facing critical system necessary to support the delivery of primary services by Rota. Primary services include Scheduling, Timekeeping, Timesheet Management, Payroll and Staff Management.	All Tier 1 systems are fully resilient and redundant across dual-data centres. The design recovery time objectives (RTO) for Tier 1 systems are a maximum of 6 hours within working hours (9am – 6pm, Monday – Friday), and a maximum of 24 hours outside of working hours. The minimum essential services for all critical systems are identified and documented. Significant projects and changes associated with these services must have documented and tested contingency plans- e.g.,

		backout plans, contingency services, extended change outage windows
2	A Tier 2 system is any other non-critical system operated or managed by Rota as a production system for Rota's operations	Tier 2 systems have a design maximum recovery time objective (RTO) of 72 working hours, and all minimum essential services are identified to ensure efficient recovery. Minimally, all Tier 2 data shall be recoverable from remote offline backup storage media, and where necessary and feasible, full systems shall be backed up. Significant projects and changes associated with these services must have documented contingency plans.

.
The assets and the systems associated with each service shall be identified and clearly defined. The owner for each service shall be assigned and the details of this responsibility documented.

Standard appropriate maintenance contracts for critical components shall be in place. In case of component or hardware replacement, vendor contacts are identified and easily accessible.

For each service, the following data shall be maintained by the Chief Operating Officer:

- Key system data: System owner, System Manager, platform details, backup mechanism, recovery mechanism, system tier ranking.
- Key operational procedures for startup, shutdown and recovery of all systems associated with the service.
- Key contacts for suppliers, SLA details or maintenance contract details where relevant, and incident invocation and escalation procedures for the supplier.
- Test schedule for system components, and full-service test schedule.

The following general data shall also be maintained:

- Contact lists for Rota's core team staff
-

The Chief Operating Officer shall be responsible for the collection, management and distribution of the DR Policy and Procedures.

System Managers and delegated systems administrators shall prepare and maintain procedures and plans as required under this policy.

Testing and Maintaining of Disaster Recovery Plans

Where possible, disaster recovery documents, specifically this policy, the procedures, and plans, shall be tested and updated to ensure that they are up to date and effective, especially following significant system changes. System level testing, including the physical hardware, is completed on a regular basis, to ensure that it operates as required and agreed with the service owner. Responsibility is assigned to system managers as identified by procedures to ensure that this is carried out in a correct manner. Operational procedures shall be reviewed by System managers after significant or major changes to underlying systems, and testing of services shall coincide with planned major upgrades.

Disaster Recovery Management and Co-ordination Policy

Disaster recovery management is incorporated in IT Services processes and structure as follows:
The activities for disaster recovery management shall be coordinated by representatives from different parts of Rota with relevant roles and job functions. This co-ordination involves the collaboration of a number of separate teams, which include the following:

1. Disaster Incident Management Team (or Management Team)
2. Recovery Action Team
3. Salvage Team
4. Communications Team

The responsibilities of each team are identified below. Where required this responsibility can be supplemented with more detailed guidance for specific disaster recovery activities. These teams with allocated responsibilities may delegate tasks to appropriate individuals; however, they shall ensure that these tasks are correctly performed. Regular meetings shall be held during the disaster, with regular updates being provided by all teams. Meeting records shall be kept documenting the decisions and actions implemented during a disaster recovery.

Disaster Incident Teams

The Disaster Incident Management Team (Management Team) shall be primarily involved in making key decisions in relation to the management of the disaster. The team shall consist of:

- Chief Executive Officer
- Chief Operating Officer
- Head of Product
- Head of People
- Others at the discretion of the management team.

This team is responsible for bringing into play the arrangements for the other teams set out below. They establish milestones and declare when disaster recovery operations are complete. This team will receive status information from the Salvage and Recovery Action teams. The handling of communication is vital if the impact of a serious incident is to be minimised and the effects of the incident on reputation are to be significantly reduced. The Management Team shall facilitate the Disaster Recovery Team in addressing, filtering, and consolidating both incoming and outgoing communication to the following distinct groups that may be affected by a disaster:

1. The Rota teams.
2. The clients and their staff.
3. Rota staff; and
4. Any other external parties.

The Management Team shall be the authoritative source for information related to the disaster. Members of all teams shall refer external queries and requests for information to the Management Team.

The Salvage Team shall immediately assemble for the purposes of implementing ad hoc actions to assess the recoverability of resources and facilities where the disaster has occurred. It is essential that the Salvage Team has activity plans, and outlines instructions to act in the various emergencies that are envisaged to allow productive engagement with the disaster. This team operates within a doctrine of understanding primary recovery objectives and current capabilities and aims to reuse remaining and existing capability to aid recovery. The Salvage Team reports to the Disaster Management Team as required. This team shall comprise:

- Chief Executive Officer.
- Head of Product.
- One or more Lead Developer(s).

The Recovery Action Team operates on the basis that the disaster will not be resolved for some time and immediately plans recovery activities in a viable location. The team shall have a detailed list of activities pre-approved to be carried out. This is particularly relevant in the first hours of a disaster. As this team's efforts are predominantly determined by planning, the team shall not in general engage in any external communication or non-recovery tasks except to the Management Team, except as necessary to perform their tasks. This team's lead shall also keep the Disaster Management Team informed of progress, status, and plans as required. The Recovery Action Team shall comprise:

- Chief Executive Officer.
- Head of Product.
- One or more Lead Developer(s) for the service impacted
- Quality Assurance

Scope of Policy

This policy applies to all Rota managed systems.