IDWEB

# DISASTER RECOVERY PLAN

# OBIETTIVI DEL DISASTER RECOVERY PLAN

- Minimize disruptions to normal operations.
- Limit the extent of disruption and damage.
- Minimize the impact of disruption.
- Establish operational arrangements in advance.
- Train personnel in emergency procedures.
- Provide for smooth and rapid restoration of service.

The Disaster Recovery Plan, has the function of explaining in detail the steps necessary for the technicians to restore the hardware and software resources used for IdSurvey service delivery.
The DR Plan also details the operational procedures necessary to make a proper assessment of the emergency/ disaster situation that does not allow the normal delivery of services by IdWeb. This document also describes the various

steps to provide for the restoration of systems, i.e., datarecovery, and the configuration of procedures to contain the emergency and initiate the subsequent return to normal operating conditions.
The Company has also provided an analysis of the possible threats and related risks that may arise from both improper management of the IT infrastructure and the integrity of electronic and IT equipment. The security and integrity of data, in terms of protecting it from various types of causes, external and internal to the Company, makes it possible to achieve levels of security that guarantee a drastic decrease in the probability of risk.
The physical integrity of computer systems, detailed in the following paragraphs, can in fact be affected or destroyed by:

- Natural disasters (floods, earthquakes, lightning, etc.).
- Accidental causes (accidents, flooding, destruction of the building, destruction of servers or other electronic processors where processed data are stored).
- External causes (riots, riots, devastation, vandalism, socio-political events, theft).

**The physical integrity of the infrastructures** is entrusted to our cloud provider, Microsoft Azure, which holds the necessary compliance certifications to ensure the quality and security of its services.

The up-to-date and complete list of certifications is available here:
https://learn.microsoft.com/en-us/azure/compliance/

**The integrity of the data**, essential for the provision of the service, must always be ensured and could be compromised by simple human errors, hardware failures, connection issues, data or access credential theft, or hacking activities. To minimize data loss or alteration, it is necessary to implement multiple layers of security and ensure proper and continuous data backup, as detailed below.

# RECOVERY PLAN

This section describes the disaster recovery solution adopted by IdWeb to ensure the continuity of IT system operation in the face of damaging events that result in service unavailability.

## RECOVERY PLAN PERSONNEL AND SKILLS

Personnel involved and authorized according to GDPR specifications.

| Name | Role | Email | Phone |
|---|---|---|---|
| Andrea Martinelli | Legal representative | andrea.martinelli@idweb.it | Make reference to the company directory. |
| Sandro Pazzi | Software Systems Manager | sandro.pazzi@idweb.it | |
| Stefano Carsena | Information Systems Manager | stefano.carsena@idweb.it | |
| Luca Pitocchi | Customer communication manager | luca.pitocchi@idweb.it | |

IdWeb applies a formal risk management method that is

updated at least once a year through in-depth audits or when major changes occur, also related to the handling of personal data and sensitive information (GDPR). This method aims to make formal the analyses performed, such as identification of resources, critical business processes, threats and vulnerabilities.
IdWeb applies a formal resource management procedure, roles and responsibilities are clearly defined.
Before each release, software updates are regularly subjected to extensive testing. intrusion tests (if applicable) can be performed. The release is rolled out gradually (1/10/100/1000) and a rollback is provided in case of risk.
Development processes are configured and monitored continuously. They contain principles for a secure development process and "privacy by design" measures.

All IdWeb services are monitored with the following objectives:

- identify production and security incidents;
- monitoring critical functions;
- forwarding alerts to staff;
- alerting managers
- initiating necessary procedures;
- ensuring the integrity of monitored resources.

IdWeb provides an incident management process to prevent, detect and resolve these types of events in the service management infrastructure and in the service itself. This process includes:

- a guide for the classification of events;
- the treatment of security events;
- testing of the incident response plan;
- communication with the customer.

These procedures benefit from a continuous improvement process for the overall monitoring, evaluation and

management of incidents and related corrective actions. Incidents are classified using the following table: the Information Systems Manager is required to use the following table to determine the severity level of the incident

| Level | Class | Descriptio | Involved staff |
|---|---|---|---|
| 1 | Ordinary | The incident does not cause significant disruption and the impact on company operations is not significant. The incident is solvable by ordinary means of intervention. | Service manager or his delegate. |
| 2 | Significant | Degradation or interruption of a minority percentage (< 25%) of the service for which the same continues to be provided even if in a slowed mode. | At the discretion of the Information Systems manager. |
| 3 | Severe | Degradation or interruption of a medium to high percentage (26% < x < 55%) of the service whereby the same continues to be delivered but causing severe disruption. | At the discretion of the Information Systems manager. |
| 4 | Disastrous | Incident causing disruption of a high to complete percentage of the service (56%<x<100%) | Legal representative Software systems manager Information Systems manager Customer communication manager" |

**The steps of the DR solution identified by IdWeb are summarized below:**

Initiating the emergency plan:

| | |
|---|---|
| 1 | Contact systems manager |
| 2 | Determine the degree of disaster |
| 3 | Contact all necessary personnel |
| 4 | Determine what actions to perform and in what sequence |
| 5 | Implement the most appropriate application recovery plan based on the extent of the disaster and, if necessary, contact the cloud service provider through the dedicated support channel. |
| 6 | Monitor progress |
| 7 | In parallel with the restoration of services alert users of the service interruption and manage communication with customers |
| 8 | Restore and declare end of emergency |
| 9 | Drafting the final report |
| 10 | Assess whether the emergency is a DataBridge and, if necessary, activate the relevant procedure |
| 11 | Assess any improvements to systems and DRP |

# SECURITY AND DATA PROTECTION

Backup is a key element in disaster recovery procedures, and to ensure higher levels of security, it is essential that data backup copies be stored outside the company's premises and the primary infrastructure providing the service.

To ensure proper backup storage, IdWeb has implemented a cloud-based infrastructure, supported by a dedicated environment and organized as follows:

- Backup files: daily snapshots are performed and retained for 30 days on zone-redundant infrastructure.
- SQL database backups: one full backup is performed weekly and retained for 14 days; one differential backup is performed daily and retained for 7 days; transaction log backups are performed every 15 minutes and retained for 7 days, all with zone redundancy.
- Virtual machines hosting SQL databases: full virtual machine snapshots are performed every 4 hours and retained for 7 days, with zone redundancy.
- Kubernetes nodes: snapshots are performed every 4 hours and retained for 7 days.
- Additional backup: a full backup is maintained on a geographically separate server farm.

IdWeb also performs periodic tests to ensure the updating and verification of backup plans. Tests are scheduled at least every six months and whenever the plan is modified.

Cloud infrastructures are constantly monitored 24/7. Any hardware malfunction detected on the services automatically triggers an intervention by the datacenter teams, who promptly replace the faulty components.

# ABOUT THE CLOUD ARCHITECTURE

For 20 years, we have been hosting our clients' data with the utmost attention to its protection. To ensure the highest possible level of security, we use effective technologies and adopt a series of best practices at every level of our organization and infrastructure.

**Datacenter Security**

- Data centers comply with industry standards such as ISO/IEC 27001:2013 and NIST SP 800-53, ensuring security and reliability.
- Physical access to servers is restricted to authorized personnel only.
- Access to datacenters is granted exclusively through multi-factor authentication systems for accredited staff.
- 24/7 video and on-site surveillance.
- Facilities equipped with smoke particle detection and fire suppression systems.
- Technical staff available 24 hours a day, 7 days a week.
- Data centers feature redundant power systems, including UPS and generators, to ensure service continuity in the event of power outages.
- Microsoft Azure complies with a wide range of international standards (ISO/IEC 27018, SOC 1/2/3, GDPR, CSA STAR, etc.), ensuring adherence to data protection regulations.

**Security and Features**

- Microsoft Azure infrastructure based on Hyper-V technology and native cloud services, with automatic updates and security patches included.
- High-performance connectivity through Microsoft's global network, providing extensive bandwidth availability.
- Support for isolated virtual networks (Azure Virtual Network) with secure and scalable subnet management.

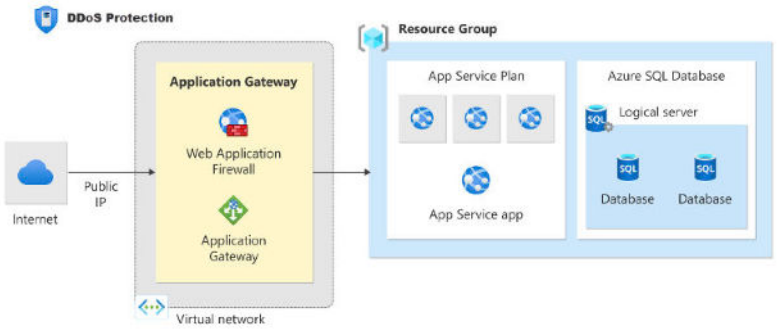
- 24/7/365 Microsoft support for incident response.
- Azure Portal and APIs for cloud resource management.
- Integrated tools for resilience testing and business continuity verification.
- Advanced monitoring services through Azure Monitor and Application Insights.
- Automated infrastructure management with transparent updates and maintenance.
- On-demand scalability of resources with rapid provisioning.
- Automatic deployment.
- Local Redundancy Storage.
- System based on internationally recognized Microsoft Azure standards.
- SSL encryption.
- Backup through Azure Backup and redundant solutions.
- Firewall and network protection via Azure Firewall, Network Security Groups, and network-level safeguards.

**Anti-DDoS PRO Protection**
With the exponential growth of online data volumes, Distributed Denial of Service (DDoS) attacks are becoming increasingly frequent.

A DDoS attack aims to make servers, applications, or entire infrastructures unavailable by overloading bandwidth or exhausting computing resources until they can no longer respond.

To ensure service continuity, Microsoft Azure integrates DDoS Protection. This protection relies on automatic mitigation techniques that enable the system to:
- analyze network traffic in real time and at high speed,
- identify and redirect malicious traffic before it reaches resources,
- filter out illegitimate packets and allow only valid traffic.

This protection is active 24/7 and leverages Microsoft's global network to ensure resilience even against large-scale attacks.




**Server Farm Certification – OnCloud Infrastructure**

The Cloud service is designed and developed according to the most rigorous international security standards, following a Security by Design and Defense in Depth approach to ensure the highest level of data protection.

Microsoft Azure adopts a transparent model and is subject to regular independent audit processes. Its security management systems are certified under ISO/IEC 27001 and comply with numerous other standards, including:

- ISO/IEC 27017 (security controls specific to cloud services),
- ISO/IEC 27018 (protection of personal data in the cloud),
- SOC 1, SOC 2, and SOC 3,
- PCI DSS (payment data security),
- CSA STAR (Cloud Security Alliance Security, Trust & Assurance Registry),
- GDPR compliance for personal data protection,
- FedRAMP and HIPAA for specific international regulatory requirements.

The up-to-date and complete list of certifications is available here: https://learn.microsoft.com/en-us/azure/compliance/

# REGULAR TESTING AND UPDATES

**Infrastructure**

Testing of the infrastructure should be carried out at least every three months. The systems manager should prepare a document with the result of the testing.

| Type | Frequency | Responsible |
|---|---|---|
| Data integrity test | Every 3 months | Software systems manager |
| Database test | Every 3 months | Software systems manager |
| Backup testing | Every 3 months | Software systems manager |
| Secondary updates | Every 3 months | Software systems manager |
| Major updates | At least once a month | Software systems manager |

**Software**

Software system testing is critical, must be performed with each release, and must reflect the following table.

| | Type | Responsible |
|---|---|---|
| 1 | Test features on local branch | Programmer |
| 2 | Test on master | Testing Team |
| 3 | Test on release | Testing Team |
| 4 | Vulnerability test on release | Software systems manager<br>Computer systems manager |
| 5 | Test release installed on client platform | Testing team |

For any further privacy and security needs, contact the security officers, legal representative, and GDPR consultants.

| Name | Role | Phone |
|---|---|---|
| Andrea Martinelli | Legal representative | Make reference to the company directory. |
| Sandro Pazzi | Software Systems Manager | |
| Stefano Carsena | Information Systems Manager | |
| Cristina Vicarelli | GDPR consultant | |
| Laura Antonelli | GDPR consultant | |