# Disaster Recovery Policy

# Table of Contents

[Purpose 3](#_Toc488132025)

[Scope 4](#_Toc488132026)

[Applicable Audience 4](#_Toc488132027)

[Compliance & Enforcement 4](#_Toc488132028)

[Policy Statements 4](#_Toc488132029)

[1. Roles and Responsibilities 4](#_Toc488132030)

[2. Disaster Recovery (“DR”) Planning 5](#_Toc488132031)

[3. Disaster Recovery Exercising 6](#_Toc488132032)

[4. Change Management 7](#_Toc488132033)

[5. Training & Awareness 7](#_Toc488132034)

[6. Maintenance and Management Reporting 7](#_Toc488132035)

[7. Business Partners 8](#_Toc488132036)

[Applicable Standards 8](#_Toc488132037)

[Related Documents 8](#_Toc488132038)

[References and Mandates 8](#_Toc488132039)

[Legal Conflicts 9](#_Toc488132040)

[Exceptions 9](#_Toc488132041)

[Document Control Information 9](#_Toc488132042)

[Revision History 10](#_Toc488132043)

## Purpose

The sustainability of client satisfaction and shareholder value relies on the continuous operation of Alight’s critical technology services. Alight has developed a framework for developing global disaster recovery plans supported through established governance and a disaster recovery policy.

The Alight Disaster Recovery Policy (“Policy”) establishes Alight’s requirements for maintaining a program that adequately prepares Alight to anticipate and respond to significant technology disruptions with protocols that protect the welfare of all Alight colleagues, business operations, reputation, image, in the interests of its shareholders and clients.

This global policy supports efficient technology recovery operations, preservation of corporate reputation, and compliance with relevant legal and regulatory requirements by mandating the necessary actions to anticipate plan for and react to an interruption of technology infrastructure, systems, services, and data.

Critical Systems and Data are the essential services and data required to meet the documented business requirements following a disaster or significant incident affecting normal business operations. Typically, Critical Systems and Data are identified utilizing the Disaster Recovery Criticality framework and the Business Impact Analysis (BIA) process completed during Business Continuity Planning.

The objectives of the Global Disaster Recovery Policy are:

* Reduce the risk of disruption of business operations or loss of information.
* Identify and prioritize the recovery of technology infrastructure, systems, services, and data and the impact of a disruption of these services.
* Formulate and implement recovery strategies and procedures to minimize impact and recover technology infrastructure, systems, services, and data.
* Administer an exercising and maintenance program to ensure viability of the strategies, services and plans.
* Ensure disaster recovery is considered and implemented as part of technology projects, migrations and other technology services.
* Ensure that recovery capability is in place with key external suppliers and/or outsource providers in the event that they are involved in a disaster.
* Ensure compliance with appropriate governance and regulatory obligations, and relevant external standards and good practices.

## Scope

The scope of this Policy is global, which includes all business units, all regions, and all entities of the Hewitt Associates LLC (“Alight”). Alight refers to all wholly-owned subsidiaries of Hewitt Associates LLC, all subsidiaries in which Alight plc has a controlling interest, and all agents or authorized representatives of Hewitt Associates LLC or its subsidiaries.

## Applicable Audience

This Policy applies to all colleagues, contractors, and vendors of Alight. The term "colleague" refers to all full-time employees, part-time employees, temporary employees, and interns who provide services to Alight. The term “contractor” refers to any individual on another company’s payroll (contactors, outsourcers, consultants, contingent workers, temporary agency workers, etc.) who provides services to Alight. The term “vendor” refers to all other third parties with which Alight does business.

## Compliance & Enforcement

Compliance with this Policy is mandatory.

Potential violations of this policy are subject to review and investigation by Alight and/or its agents. Violations of this policy may result in discipline, up to and including removal of assignment, end of contract for vendors or termination. This is subject to the procedural requirements of the countries in which Alight operates. Alight reserves the right to refer for prosecution any violations of this policy.

This Policy constitutes the current Policy with respect to its subject matter, and it supersedes and replaces all previous policies relating to its subject matter. Alight reserves the right to modify the Policy at its sole discretion at any time with the intent to update on an annual basis.

## Policy Statements

### Roles and Responsibilities

* 1. Alight Global Business & Technology Resilience Program Office

The Alight Global Business & Technology Resilience Program Office (“BTR Program Office”) is the global governing body for Disaster Recovery Planning. The Global BTR Program Office is responsible for providing guidance and standardized frameworks for disaster recovery plan development, maintenance, and exercising and for providing and maintaining a solution for centralized plan retention. The BTR Program Office will provide periodic status reports to senior management on the progression of disaster recovery plan development, maintenance, and exercising.

* 1. Alight Information Technology Services Global Disaster Recovery

Develops and maintains AITS Disaster Recovery plans in accordance with the Alight DR policy including coordination, execution and reporting on AITS led DR exercises and planning activities.  In support of the broader Alight business DR program, AITS global DR consults with the business technology organizations, where applicable, on DR strategies for internally and 3rd party hosted applications and services.

* 1. Alight Businesses

All businesses within Alight are responsible for developing, maintaining, and exercising disaster recovery plans that adhere to the policy and standards set forth by Alight’s BTR Program Office.

Each business unit is responsible for identifying key individuals and succession plans to ensure the following disaster recovery management, delivery, and support roles are filled.

Each business unit is responsible for identifying key individuals and succession plans to ensure the following business continuity management, delivery, and support roles are filled.

* + 1. C-Level Executive or Country Manager has overall responsibility for the strategic and operational management of the organization and will serve as the DR Program sponsor, is the ultimate decision maker over budget, and is accountable for all disaster recovery planning within all business units under their authority.
    2. Executive Business Leader: is the executive sponsor within a specific business and is responsible for determining planning/recovery budget, prioritizing critical services/systems, identifying plan owners, and approving recovery strategies. They will also be a decision maker in the execution of disaster recovery plans.
    3. Executive Plan Owner: must be of management level and is responsible for the development and management of disaster recovery plan(s). They are required to participate in annual exercises and plan sign-off and will be responsible for executing recovery strategies in the event of a significant technology disruption.
    4. Plan Coordinator: is responsible for coordinating the development and management of disaster recovery plan(s). They are required to participate in annual exercises and publishing plan documentation. The plan coordinator may also be called upon to assist in the execution of recovery strategies in the event of a significant technology disruption.
    5. All Staff: are responsible for cooperating with the implementation of this Policy as part of their normal duties and responsibilities or as assigned within specific disaster recovery plans.

### Disaster Recovery (“DR”) Planning

* 1. All identified Alight infrastructure, systems and services must have Disaster Recovery plans to ensure swift, organized, and coordinated responses to technology interruptions.
  2. Each business unit must evaluate current critical infrastructure, systems, and services and implement strategies to reduce exposure or risks to foreseeable incidents that may impact critical technology supporting business operations.
  3. Each business unit must ensure DR is adequately funded and resourced to deliver key planning, maintenance, exercising and reporting activities.
  4. Each business unit must comply with the Alight Disaster Recovery Standard for the production of a Disaster Recovery plan with the following components, at a minimum, but not limited to
     1. Recovery Strategy Overview
     2. Application Description
     3. Application Criticality Tier
     4. Production Location
     5. Recovery Location
     6. Recovery Time Objective
     7. Recovery Point Objective
     8. Disaster Recovery Team
     9. Interdependencies
     10. Detailed Recovery Procedure
     11. Plan Maintenance
  5. Each business unit must review the adequacy and currency of the DRPs and their DR solutions annually or when a major change takes place.
  6. All new systems, services, or infrastructure must have a viable DR position before the go live and should be exercised as part of the project/migration plan. In cases where this is not possible before go-live, an approved exception must be on file.

### Disaster Recovery Exercising

* 1. All DR plans must be exercised on an annual basis to verify that the disaster recovery capabilities meet or exceed the recovery times required by the business.
  2. All systems in Alight’s DR portfolio must have an annual disaster recovery exercise schedule on file with the Alight BTR Program Office
  3. All DR exercise plans must include clearly defined and agreed upon objectives, as well as a list of success criteria for the exercise.
  4. Any risks posed by DR exercising must be identified and assessed prior to any DR exercise to ensure that there is no unplanned disruption to the production environment.
  5. Each critical system must have a fully documented and approved exercise plan utilizing Alight’s DR exercise framework or approved outsource vendor framework completed prior to the exercise.
  6. DR exercise documentation must be signed off by all parties concerned.
  7. Each critical system must have documented exercise results utilizing Alight’s DR exercise framework or approved outsource vendor framework.
  8. Responsible parties for each critical system must remediate and update DRPs in accordance with any deficiencies or issues discovered during the annual exercise.
  9. Production services/business as usual activities take preference over exercising, and exercises may be rescheduled where the integrity of the production services is threatened or due to an urgent business requirement.

### Change Management

* 1. Where applicable, all Information Technology change management requests must clearly state the impact(s) of the stated changes on the current disaster recovery capabilities.
  2. Where applicable, all Information Technology change management activities must ensure that existing DRPs are updated to reflect the change.
  3. All changes must comply with the appropriate Information Technology change management policy.

### Training & Awareness

* 1. This policy shall be made available to all Alight colleagues.

### Maintenance and Management Reporting

* 1. All DR plans will be developed, maintained, and stored in Alight’s online Continuity & Analytics Management (“CAM”) Tool, [https://enterprise.sungardas.com](https://enterprise.sungard.com/), the Alight SharePoint Sites (one.Alight.net), or approved vendor plan management system or in a globally approved alternate format.
  2. Regional Business & Technology Resilience leaders should be notified of any material changes that occur to disaster recovery operations, strategies or plans. This includes, but is not limited to creating or removing plans, applications, systems, services or operating locations.
  3. Regular compliance reporting will be generated by the BTR Program office utilizing the online CAM Tool to create awareness and drive development, exercising and maintenance of business continuity plans according to this Policy.

### Business Partners

* 1. Third-party Information Technology outsource providers must demonstrate DR capability though appropriately documented and exercise strategies and plans ensuring that plans are ‘fit for purpose’ and that they can recover/continue to deliver services at a level acceptable to Alight.
  2. Third party suppliers must have DR arrangements in place. These arrangements should ensure that they are able to continue to provide services and support to Alight in the event of a disruption that affects their business.
  3. Third-party Information Technology outsource partners must ensure their DR plans are compatible with Alight’s plans and strategies, and specifically detail an agreed upon notification and escalation process with Alight, roles and responsibilities, and clear procedures for crisis management.

## Applicable Standards

* None

## Related Documents

* Business Continuity Management Policy

## References and Mandates

* SEC 17 CFR 240 (2005) – SEC regulations require that financial transaction histories be maintained for all electronic securities transactions, and backup power be in place to maintain continuity. This regulatory requirement is mandatory for applicable entities.
* GLBA: Gramm-Leach-Bliley Act (1999) – Applies to all US financial institutions, which include not only banks, securities firms, and insurance companies, but also companies providing many other types of financial products and services to consumers.
* NYSE Rule 446 / NASD 3510/3520 (2004) – Applies to all members and member organizations of the NYSE or NASD.
* ISO/IEC 22301:2014; Societal security. Business continuity management systems. Requirements
* ISO/IEC 27001:2013; Information technology - Security techniques - Information security management systems – Requirements
* COBIT 5: Control Objectives for Information and related Technology
* Framework for Improving Critical Infrastructure Cybersecurity; Version ; NIST; 12 February 2014

## Legal Conflicts

Alight’s Security Policies and Standards were drafted to address the protections found in existing laws and regulations and may be amended as necessary due to law, regulation, or business requirements. There is no intent to conflict with relevant local laws or regulations. In the event of any conflict with relevant local laws or regulations, they will control.

Alight’s Security Policies and Standards may be supplemented by other policies or standards of Alight. In the case of a conflict or ambiguity, the more specific provisions of any such policy or standard shall take precedence over the more general provisions contained in Alight’s Security Policies and Standards.

## Exceptions

Exceptional circumstances occur from time to time. In these situations, contact Alight Global Security Services at [global.security.services@Aon.com](mailto:global.security.services@aon.com) for further guidance.

## Document Control Information

Document Control Information

|  |  |
| --- | --- |
|  |  |
| Primary Contact | Alight Global Security Services | [global.security.services@Aon.com](mailto:SRM.Mailbox@aon.com) |
| Version Number | 1.5 |
| Owner | Alight Global Security Services | Global Business & Technology Resilience |
| Author(s) | Alight Global Security Services | Global Business & Technology Resilience |
| Approved By | Jim Hartley, Chief Information Security Officer |
| Approval Date | May 1, 2017 |
| Effective Date | May 1, 2017 |
| Creation Date | May 2, 2011 |
| Information Classification | General Internal – Low Business Impact (Green) |

## 

## Revision History

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Revision Level | Date | Description | Change Summary |
| 1.0 | 2012 March | Original | Restructured policy due to Aon Hewitt acquisition |
| 1.1 | 2013 June | 2013 Annual Review | Changed wording 1.2 to AITS  Deleted 5.2  Changed wording Section 6 |
| 1.2 | 2014 July | 2014 Annual Review | Reviewed and validated |
| 1.3 | 2015 July | 2015 Annual Review | Updated wording in 3.4, 3.6 and 6.1  Added references to References and Mandates Section |
| 1.4 | 2016 July | 2016 Annual Review | Replaced all instances of Global Business Continuity Management / Disaster Recovery (GBCM/DR) with Global Business & Technology Resilience to reflect the new team name. Also, replaced all instances of Security Risk Management (SRM) with Global Security Services (GSS) to reflect new organizational name. |
| 1.5 | 2017 May | 2017 Rebranding | Rebranded policy due to Aon Hewitt divestiture |
|  |  |  |  |