# Physical Security Audits and Compliance Standard

Related Policy

* 300.00 Physical Security Policy

Purpose

The purpose of this standard is to ensure that effective physical access controls are present at every Alight office location. Effective physical access control includes the use of people, technology, policies and procedures to secure Alight space from unauthorized persons. Physical access controls reduce the risk to Alight colleagues, work product and client information.

Audits & Compliance is the process by which internal surveying and testing measures are taken to assess the presence, effectiveness, and accordance of physical security policies and controls.

Standard Statements

### Audits and Compliance

* 1. Alight’s Global Security Services (GSS) maintains an internal team, which is responsible for supporting Alight’s compliance with Service Organization Controls (“SOC”), Sarbanes-Oxley regulations (“SOx”), Payment Card Industry (PCI) and other regulations (may vary by region and country) regarding physical security controls.
     1. Alight’s Internal Audit measures/tests GSS’ execution of established building physical security access policies and procedures.
     2. GSS is required to support and assist with Alight’s internal audit program.
  2. Alight has commissioned an external auditing firm for testing Alight and GSS’ compliance with established physical security controls.
     1. The auditor provides independent third-party verification regarding Alight’s assertion that the defined controls are in place and operating effectively.
     2. The auditor provides Alight and specified clients the Service Organization Controls (“SOC”) based on their independent assessment of compliance with the established controls at the established Alight office locations.
     3. Alight GSS Global Protection Services (GSS GPS) is required to support and assist with the assessment of the following five (5) physical security controls:
        1. Security devices (e.g., an electronic keycard system) control access to facilities.
        2. Keycards are coded to only allow access to areas necessary to perform job functions.
        3. Sensitive data processing areas (i.e., data rooms housing servers that support client applications, routers, check printing rooms, or other communications equipment) are restricted to the appropriately authorized individuals.
        4. Access to sensitive data processing areas is subjected to periodic access reviews.
        5. For terminated Alight colleagues, keycard access is removed on a timely basis.
     4. The five (5) controls are assessed periodically as coordinated by the independent auditor and Alight Internal Audit.
     5. Alight is responsible for quarterly assertions attesting that physical security controls are in place and operating effectively. Any changes in the controls are communicated at the time of the assertion.

Communications

Questions regarding this Standard should be directed to GSS GPS at [global.security.services@aon.com](mailto:global.security.services@aon.com).

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 of Alight shall take precedence over the more general provisions contained in Alight’s Security Policies and Standards.

Exceptions

Application of the global physical security policies and standards may vary by region and office, and exceptions and variations may occur, if and when approved by GSS GPS. Please contact GSS GPS at [global.security.services@aon.com](mailto:global.security.services@aon.com) for further guidance on any exceptions or variations that may apply.

Applicable Standards

* None

# References & Mandates

* SSAE 16—Statement on Standards for Attestation Engagement No. 16
* ISAE 3402—International Standard on Assurance Engagements No. 3402

# Document Control Information

Document Control Information

|  |  |
| --- | --- |
|  |  |
| Primary Contact | Alight Global Security Services | [global.security.services@aon.com](mailto:global.security.services@aon.com) |
| Version Number | 1.6 |
| Owner | Alight Global Security Services | Global Protection Services |
| Author(s) | Alight Global Security Services | Global Protection Services |
| Approved By | Jim Hartley, Chief Information Security Officer |
| Approval Date | May 1, 2017 |
| Effective Date | May 1, 2017 |
| Creation Date | May 1, 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 | Reviewed and validated |
| 1.2 | 2014 June | 2014 Annual Review | Reviewed and validated |
| 1.3 | 2015 June | 2015 Annual Review | Reviewed and validated |
| 1.4 | 2016 June | 2016 Annual Review | Clarified wording and replaced all instances of Security Risk Management (SRM) with Global Security Services (GSS) to reflect new organization name |
| 1.5 | 2017 January | 2017 Update | Name change from Corporate Protection Services (CPS) to Global Protection Services (GPS) |
| 1.6 | 2017 May | 2017 Rebranding | Rebranded policy due to Aon Hewitt divestiture |
|  |  |  |  |