# Incident Response Standard

## Related Policy

* 208.00 Incident Response Policy

## Purpose

This Standard covers incidents that may affect the confidentiality, integrity, and availability of Alight's information assets and documents the key requirements for effectively addressing an information security incident.

This Standard is not intended to provide a substitute for legal advice but approaches the topic from an information security perspective.

## Standard Statements

### Computer Security Incident Response

Six steps are to be followed on any computer security related incident or any major threat that could imminently impact operating systems within Alight Corporation:

* 1. **Preparedness** – prevent the incident. This step will ensure Alight will take all appropriate actions to protect the infrastructure, including: colleague awareness training, hardening of operating systems, installation of security tools, and the documentation of specific policies and procedures. Additionally, Alight requires an annual incident response test to validate that colleagues know the appropriate IR procedures and understand the required steps in the IR process.
  2. **Identification** – identify possible attack symptoms. This step will monitor systems for symptoms that characterize a possible attack.
  3. **Containment** – isolate the attack to prevent it from spreading. This step will limit the scope and magnitude of a threat or security incident.  A decision will be made as to whether the system will be shut down entirely, disconnected from the network, or be allowed to continue running in normal operation so that any activity on the system can be monitored.  If the system is highly sensitive, contains critical information, or hosts programs that may be at risk, the Computer Security Incident Response Team (IRT) lead by AC3 will make the determination with the appropriate leadership input to shut down the system and isolate it from the network.
  4. **Eradication** – defeat the attack. This step will eliminate components of the incidents, such as deleting malicious code and disabling compromised user accounts.  The primary goal will be to restore systems to normal operations and (if applicable) harden systems to prevent similar future incidents.
  5. **Recovery** – restore systems. This step will restore a system back to its normal operational status. The IRT will employ the following actions to recover an impacted system:
     1. Restoring system from clean backups.
     2. Rebuilding systems from scratch.
     3. Replacing compromised files.
     4. Installing patches.
     5. Changing passwords.
     6. Increase the level of logging and monitoring.
     7. Tightening host based and network perimeter security.
  6. **Lessons Learned** – determine what actions can be taken to prevent the attack in the future. This step will document improvement areas identified by the IRT led by AC3 using a fact-based approach to evaluating the incident as a whole. These improvements will reduce the possibility of a similar attack’s effectiveness in the future.

### Team Composition

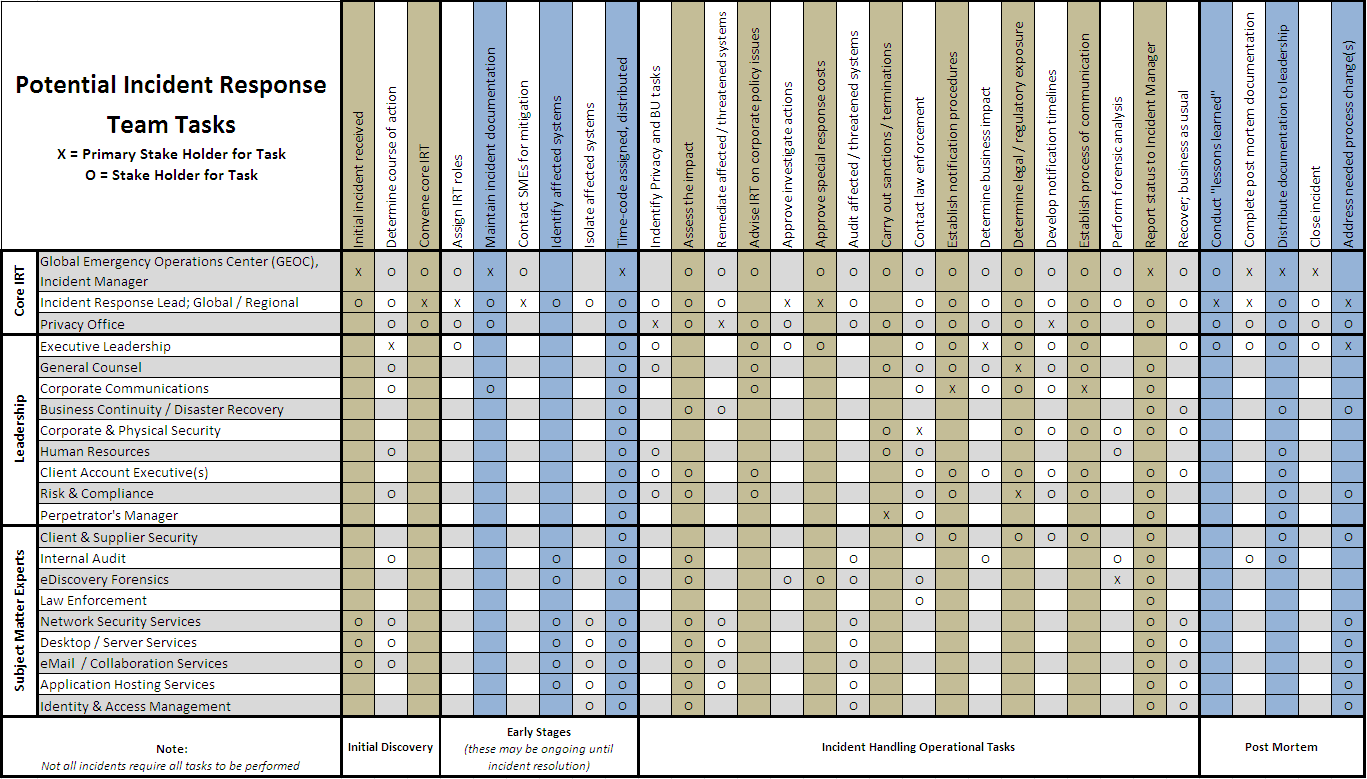
* 1. The composition of the team is dynamic and will be determined by the nature of the incident.
     1. Not every information security incident may require participation of all Computer Security Incident Response Team members.
  2. A Computer Security Incident Response Team (IRT) is comprised in such a way as to provide a well-defined organizational approach to handling any potential security threat to Alight's computers and/or data.  It is created to provide an effective and orderly response to containing, mitigating, and eventually resolving security incidents.  Upon an information security incident, each team member will follow their pre-established escalation processes, which may vary based on business practice.  Within Alight, the AC3 will be the lead for the IRT.
  3. Roles and Responsibilities of the Core Incident Response Team:

| **Role** | **Responsibilities** |
| --- | --- |
| Global Emergency Operations Center / Incident Manager | * Central point of contact for communications both internal and external, with the assistance of the Privacy Office * Determines which core members to involve in the incident based on type / scale * Responsible for coordinating, tracking, and reporting on the status of an incident |
| Alight Cybersecurity Command Center (AC3) | * A member of Global Security Services, responsible for identifying and directing additional resources needed to address the incident * Provides analysis on the information security incident; proposes next steps alongside business application experts * Assesses the need for change to policies, procedures, and standards as a result of any incident |
| Privacy Office | * Monitors all communications regarding the incident * Advises on next steps with respect to regulations and contractual obligations * Works with client account executives in the event a data breach is involved |

* 1. Potential Incident Response Team Composition with Incident Type:
  2. Each of the areas listed in the above table will have a primary and secondary colleague listed as a contact.  Contact data is provided for each team within the Global Systems Operation Center database, and is updated weekly by each team for on-call purposes.

### Incident Response Team Tasks

* 1. Each team member involved in investigating an information security incident will perform certain actions to remediate the situation as appropriate to the incident response as outlined in the following table.



### Forensic Analysis

In certain computer security incidents, forensic analysis will have to be performed in order to fully understand the overall scope of the incident.  Often times, forensics may simply be the steps taken to contain the incident.  Forensic analysis will be conducted by a resource designated by the IRT and will depend on the nature of the attack. The data / information obtained through any investigation will be considered confidential in nature, and will be shared with leadership only, and only on a need-to-know basis.

* 1. In certain instances, a third-party vendor may be brought in to perform the exhaustive forensic analysis.  The Incident Lead, a member of Global Security Services AC3 team, will make this determination.
  2. The goals described below are to ensure the information obtained can be used for later litigation if necessary.
     1. Establish a chain of custody for all assets affected by the incident.
     2. Provide a complete list of all affected devices, accounts, etc. including exact time of the incident for analysis, as well as any potential entry points.
     3. Determine who had legitimate access to the affected components prior to the incident.
     4. Secure all formal backups and record all backup procedures, as well as all logs.
     5. Collect and secure any informal backups on removable media and write-protect them; additionally, physically remove and secure them.
     6. Image and backup any drives or removable media to tamper-proof media, such as a CD-R or DVD-R (but not a CD-RW or DVD-RW).
     7. By utilizing proper imaging techniques, the information collected through forensic analysis will be in a format suitable for a court of law in the event a criminal investigation is warranted. The eDiscovery and Forensics team will lead the effort to ensure those standards are met.
     8. Document all steps taken by every person involved, including exact time and date.
  3. All assets that have been identified as within scope of a forensics investigation are to be immediately quarantined in a secure location and no action is to be taken on the impacted device by anyone other than a member of the Forensics Team.
     1. Certain actions can take place (such as removing the drive to prepare it for shipping or secure storage) before forensic analysis.
     2. Identifying an impacted device will occur through various means, such as IP address, host name, asset management, or simply association with other impacted assets.
  4. It is the responsibility of the Global Security Services team to communicate to the technology organization when assets are to be quarantined, and to what extent.
  5. Assets marked for forensic investigation will remain within the custody of the forensics team until it is no longer deemed necessary.
  6. Assets that become part of an ongoing investigation, or are considered legal evidence, shall remain in custody for a period of two (2) years, unless instructed otherwise by General Counsel and/or the Privacy Office.

### Post Incident Tasks

* 1. Every computer security incident will have a follow-up meeting to discuss the events of the incident, and ultimately, what Alight Colleagues can do in the future to mitigate the potential risk from reoccurring.  The goal of these meetings is to determine root-causes and work to continuously improve the confidentiality, integrity, and security of Alight’s information assets. The goals of these meetings include, but are not limited to, the following:
     1. Gather the designated Computer Security Incident Response Team, preferably within 10 days of incident closure.  Information that will be gathered in these meetings will, at minimum, include:
        1. A description of the incident including when and what happened.
        2. Staff and management performance when dealing with the incident.
        3. A review of steps that were performed during the incident and a comparison of the activities vs. this standard.
        4. A review of the information gathered including the timeliness of the information gathered and how effective it was in managing the incident.
        5. Barriers that reduced the effectiveness of the incident response.
        6. Future improvements and prevention strategies that can be implemented.
        7. Additional tools or resources needed to detect, analyze, and mitigate future incidents.
     2. Conduct a root-cause analysis of the computer security incident.
     3. Evaluate and review the tracking log of the incident, which is available within the security incident documentation held by GEOC.
     4. Evaluate and review the forensic analysis that has been performed, if applicable.
     5. Report findings to business unit CIOs, as well as anyone impacted by the event.
     6. Make appropriate requests for enhancements needed, if any, to further secure the environment.

### Incident Documentation and Reporting

* 1. All relevant aspects of an information security incident will be documented and reported to the appropriate authorities in a timely fashion including a documented root cause analysis.
  2. The IRT will determine what information needs to be recorded, timelines for report submission, report recipients, and report retention based on the specifics of the incident.
  3. Alight will use the defined GEOC incident communication strategy to report incident information to customers, Alight colleagues, and the media. Factors for consideration when assessing communications should include:
     1. The total number of persons impacted.
     2. The sensitivity of the information released.
     3. Additional risks to the information associated with public communication of the event, customer/colleague expectations.
     4. Regulatory requirements.
  4. Alight will use the defined GEOC communication strategy to send notices that may be required to outside entities such as federal or state regulatory authorities, law enforcement agencies, industry organizations (e.g., VISA/MasterCard), or by contract to other outside parties (e.g., service providers).
     1. Prior to notification, the appropriate Legal and business unit CIO approvals will be obtained.

## References and Mandates

* Payment Card Industry DSS

## Legal Conflicts

Alight 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 laws or regulations. In the event of any conflict with relevant laws or regulations, they will control.

Alight 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 Security Policies and Standards.

## Document Control Information

Document Control Information

|  |  |
| --- | --- |
| Document Name | 208.01 Incident Response Standard |
| 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 | Information Security |
| Author(s) | Alight Global Security Services | Information Security |
| 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 due to Aon Hewitt merger |
| 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 | 2015 November | Update Wording | Added wording for Security Operations Center roles and responsibilities |
| 1.5 | August 2016 | 2016 Annual Review | Updated name change from IRSS with Global Security Services (GSS) to reflect new organization name. |
| 1.6 | 2017 July | 2017 Rebranding | Rebranded policy due to Aon Hewitt divestiture |
|  |  |  |  |