



# Security Incident Management in Microsoft Office 365

Published: November 29, 2016



---

*This document describes how Microsoft handles security incidents in  
Microsoft Office 365*

---

## Introduction

Microsoft works continuously to provide highly secure, enterprise-grade services for Office 365 customers. This document describes how Microsoft handles security incidents in Office 365. A security incident refers to any unlawful access to customer data stored on Microsoft's equipment or in Microsoft's facilities, or unauthorized access to such equipment or facilities that has the potential to result in the loss, disclosure, or alteration of customer data. Microsoft's goals when responding to security incidents are to protect customer data and the Office 365 services.

The Office 365 Security team and the various service teams work jointly and take the same approach to security incidents: Preparation; Detection and Analysis; Containment, Eradication, and Remediation; and Post-Incident Activity.

## Microsoft Approach to Security Incident Management

Microsoft's approach to managing a security incident conforms to [National Institute of Standards and Technology](#) (NIST) Special Publication (SP) 800-61, and Microsoft has several dedicated teams that work together to prevent, monitor, detect, and respond to security incidents. The teams discussed in this document are described in Table 1.

Team	Description
<b>Microsoft Security Response Center (MSRC)</b>	Identifies, monitors, resolves, and responds to security incidents and Microsoft software security vulnerabilities.
<b>Corporate, External, and Legal Affairs (CELA)</b>	Provides legal and regulatory advice in the event of a suspected security incident.
<b>Office 365 Security Incident Response</b>	Partners with Office 365 Service teams to build the appropriate security incident management process and to drive any security incident response.
<b>Office 365 Trust Service teams</b>	Provides guidance on regulatory requirements, compliance and privacy. Engineering teams for Office 365 services, such as Exchange Online, SharePoint Online, and Skype for Business, that are responsible for security-related policies and decisions for each service.
<b>Online Services Security and Compliance (OSSC)</b>	Provides security operations for Microsoft's datacenters and network infrastructure. OSSC is part of the Cloud & Enterprise division at Microsoft, and a key Office 365 security response partner.
<b>Microsoft Threat Intelligence Center (MSTIC)</b>	Provides the current state of art in digital security threats against Microsoft infrastructure and assets, helps partner teams inside Microsoft prioritize mitigation and prevention effort action plans, and increases protection by adopting near real-time incident monitoring/detection.
<b>Partner Security teams</b>	Other partner security teams inside Microsoft that provide key services or are responsible for key dependencies in Office 365, such as the Azure Security Response team and the OSSC team.
<b>Office 365 Customer Experience (CXP) Communications</b>	Engineering team responsible for all customer communications about security and service incidents.

Table 1 - Teams involved in Microsoft's security incident response management

Some service teams also work with additional security stakeholders as part of their incident management process. For example, the Yammer Security Operations (YSO) team works with several service-specific teams, which are described in Table 2.

Team	Description
<b>Director of Security</b>	Engineering executive responsible for directing incident response activities for Yammer applications and systems
<b>First Responder</b>	Yammer representative that acts as primary contact for incident reports, and a triage point for inbound issues
<b>QA Lead</b>	A Quality Assurance engineering lead that certifies a security patch as having been tested and ready to deploy
<b>Cross Functional Security Team (CST)</b>	A team composed of senior representatives from Yammer Engineering, Customer Support, and CELA who collaborate to implement Yammer's Information Security Management System.
<b>Yammer Security Operations</b>	Works with the MSRC to drive incident and breach response readiness, security incident detection, and security incident response in a predictable manner.

Table 2 - Additional teams that work with Yammer Security Operations

## Response Management Process

The Office 365 Security team and the service teams work together on and take the same approach to security incidents, which is based on the NIST 800-61 response management phases:

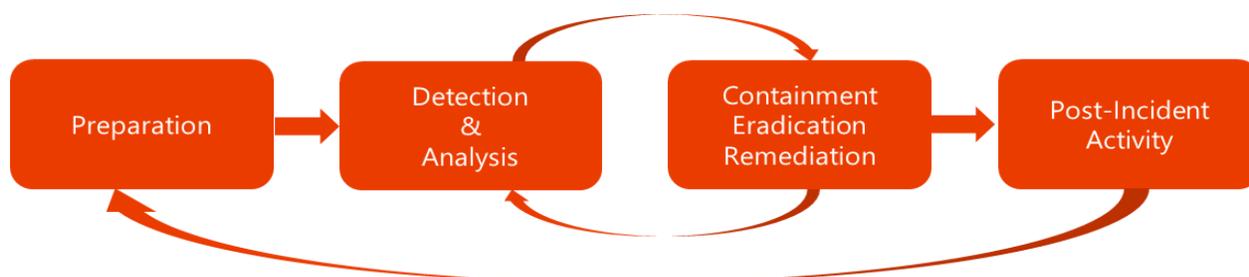


Figure 1 - NIST 800-61 Response Management Phases

- **Preparation** Refers to the organizational preparation that is needed to be able to respond, including tools, processes, competencies, and readiness.
- **Detection & Analysis** Refers to the activity to detect a security incident in a production environment and to analyze all events to confirm the authenticity of the security incident.
- **Containment, Eradication, Remediation** Refers to the required and appropriate actions taken to contain the security incident based on the analysis done in the previous phase. Additional analysis may also be necessary in this phase to fully remediate the security incident.
- **Post-Incident Activity** Refers to the post-mortem analysis performed after the remediation of a security incident. The operational actions performed during the process are reviewed to determine if any changes need to be made in the Preparation or Detection & Analysis phases.

## Federated Security Response Model

Office 365 services include core Microsoft Online Services (Exchange Online, SharePoint Online and Skype for Business, etc.) as well as other Microsoft cloud services, such as Azure Active Directory, the Microsoft Commerce Platform, and the MSTIC. These services are operated by separate teams with their own security operational processes. Other Microsoft teams are also engaged in various security aspects of Office 365. Because of the multitude of teams working on security operations management for Office 365, Microsoft has implemented a federated security response model.

Table 3 presents the operational boundaries between the various Office 365 security operations teams and the Office 365 service teams:

Activity	Office 365 Security Team Operations	Office 365 Service Team Operations
Detection & Analysis	<ul style="list-style-type: none"> <li>▪ Detection requirements</li> <li>▪ Security monitoring and analysis</li> <li>▪ Indicators of compromise (IOC) sweeps</li> <li>▪ Breach hunt</li> <li>▪ 24x7 security on-call/Incident Response lead</li> </ul>	<ul style="list-style-type: none"> <li>▪ Detection requirements</li> <li>▪ Monitoring infrastructure deployment</li> <li>▪ Service analysis and insight</li> <li>▪ Event and alert triage</li> <li>▪ 24x7 service engineering on-call</li> </ul>
Containment Eradication Remediation	<ul style="list-style-type: none"> <li>▪ Incident response lead</li> <li>▪ Forensics investigation</li> <li>▪ Security expertise and consult</li> <li>▪ Remediation guidance</li> </ul>	<ul style="list-style-type: none"> <li>▪ Security incident owner</li> <li>▪ Service insight and expertise</li> <li>▪ Execute containment, eradication, remediation</li> </ul>
Post-Incident Activity	<ul style="list-style-type: none"> <li>▪ Post-Incident analysis lead</li> <li>▪ Data collection and archival</li> <li>▪ Lessons learned and bug requests</li> <li>▪ Incident reporting</li> </ul>	<ul style="list-style-type: none"> <li>▪ Service-side incident analysis</li> <li>▪ Prioritize follow-up activities</li> <li>▪ Implement security investments</li> <li>▪ Service security readiness</li> </ul>

Table 3 - Operational boundaries between Office 365 security teams and service teams

## Preparation

### Training

Each employee working on Office 365 is provided with training regarding security incidents and response procedures that are appropriate to their role. Every Office 365 employee receives training upon joining, and annual refresher training every year thereafter. The training is designed to provide the employee with a basic understanding of Microsoft's approach to security so that upon completion of training, all employees understand:

- The definition of a security incident;
- The responsibility of all employees to report security incidents;
- How to escalate a potential security incident to Office 365 Security Incident Response team;
- How the Office 365 Security Incident Response team responds to security incidents;
- Special concerns regarding privacy, particularly customer privacy; and
- Where to find additional information about security and privacy, and escalation contacts.

Annually, the appropriate employees receive refresher training on security. The annual refresher training focuses on:

- Any changes made to the Standard Operating Procedures in the preceding year;
- The responsibility of everyone to report security incidents, and how to do so; and
- Where to find additional information about security and privacy, and escalation contacts.

Moreover, each employee working on Office 365 goes through an appropriate thorough background check that includes the candidate's education, employment, criminal history, and other specific information per United States regulations like HIPAA, ITAR, FedRAMP, and others. The background checks are mandatory for all employees working within Office 365 engineering. Some Office 365 environments and operator roles may also require full fingerprinting, citizenship requirements, and other more stringent controls. In addition, some service teams go through specialized security training.

### Compliance Control

The Office 365 Security team also develops guidance on compliance, security and privacy. All service teams use the Security team's guidance to setup the appropriate security and compliance controls inside of Office 365.

### Security Development Lifecycle

The Security Development Lifecycle (SDL) is a software development process that helps developers build more secure software and address security compliance requirements while reducing development costs. In January 2002, many Microsoft software development groups prompted "security pushes" to find ways to improve existing security code. Under this directive, the Trustworthy Computing team at Microsoft formed the concepts underlying the SDL that has since continually evolved and improved.

Established as a mandatory policy in 2004, the SDL is an integral part of the software development process at Microsoft. The development, implementation, and constant improvement of the SDL represents a strategic investment in security. This was an evolution in the way that software is designed, developed, and tested, and it has matured into a well-defined methodology. Our commitment for a more secure and trustworthy computing

ecosystem has also led to the creation of guidance papers, tools, and training resources that are available to the [public](#).

## Penetration Testing

Microsoft works with a variety of industry bodies and security experts to understand new threats and evolving trends. Microsoft continuously assesses its own systems for vulnerabilities, and contracts with a variety of independent, external experts who do the same. The tests carried out for service hardening within Office 365 can be grouped into four general categories:

1. **Automated security testing** Internal and external personnel regularly scan the Office 365 environment based on Microsoft SDL practices, Open Web Application Security Project (OWASP) Top 10 risks, and emerging threats reported by different industry bodies.
2. **Vulnerability assessments** Formal engagements with independent, third-party testers regularly validate whether key logical controls are operating effectively to fulfill the service obligations of various regulatory bodies. The assessments are carried out by Council of Registered Ethical Security Testers (CREST)-certified personnel and are based on OWASP Top 10 risks and other service-applicable threats. All threats found are tracked to closure.
3. **Continuous system vulnerability testing** Microsoft carries out regular testing in which teams attempt to breach the system using emerging threats, blended threats, and/or advanced persistent threats, while other teams attempt to block such attempts to breach.
4. **Microsoft Online Services Bug Bounty Program** This program operates a policy of allowing limited, customer-originated, vulnerability assessments on Office 365. For more information, see [Microsoft Online Services Bug Bounty Terms](#).

The Office 365 engineering team publishes a yearly internal document describing the security and legal-related improvements made to Office 365 during the last calendar year that are designed to help customers and partners meet legal requirements surrounding independent verifications and audits of Office 365. That document is available, under a non-disclosure agreement, from the [Microsoft Cloud Service Trust Portal](#) (STP)<sup>1</sup> and from the Service Assurance area of the [Office 365 Security & Compliance Center](#).<sup>2</sup>

## Wargames

Microsoft engages in ongoing wargames exercises and live-site penetration testing of our security and response plans with the intent to improve detection and response capability. Microsoft regularly simulates real-world breaches, conducts continuous security monitoring, and practices security incident response to validate and improve the security of both Office 365 and Azure.

Microsoft executes an assume breach security strategy using two core teams:

- Red Teams (attackers)
- Blue Teams (defenders)

Both Azure and Office 365 staff have separate full-time red teams and blue teams. Referred to as *Red Teaming*, the approach is to test Azure and Office 365 systems and operations using the same tactics, techniques and

---

<sup>1</sup> See [Get started with the Service Trust Portal for Office 365 for business, Azure, and Dynamics CRM Online subscriptions](#) for details on how to access the STP.

<sup>2</sup> An Office 365 subscription is required to access the Office 365 Security & Compliance Center.

procedures as real adversaries, against the live production infrastructure, without the foreknowledge of the infrastructure and platform engineering or operations teams. This tests security detection and response capabilities, and helps identify production vulnerabilities, configuration errors, invalid assumptions or other security issues in a controlled manner. Every Red Team breach is followed by full disclosure between the Red Team and Blue Team to identify gaps, address findings and significantly improve breach response.

**Note** No customer data is deliberately targeted during Red Teaming or live site penetration exercises. The tests are against Office 365 and Azure infrastructure and platforms, as well as Microsoft's own tenants, applications and data. Customer tenants, applications and data hosted in Office 365 or Azure are never targeted.

## Red Teams

The Red Team is a group of full-time staff within Microsoft that focuses on breaching Microsoft's infrastructure, platform, and Microsoft's own tenants and applications. They are the dedicated adversary (a group of ethical hackers) performing targeted and persistent attacks against online services (but not customer applications or data). They provide continuous "full spectrum" validation (e.g. technical controls, paper policy, human response, etc.) of service incident response capabilities.

## Blue Teams

The Blue Team is comprised of a dedicated set of security responders, as well as members from across the security incident response, engineering, and operations teams. They are independent and operate separately from the Red Team. The Blue Team follows established security processes and uses the latest tools and technologies to detect and respond to attacks and penetration attempts. Just like real-world attacks, the Blue Team does not know when or how the Red Team's attacks will occur or what methods may be used. Their job, whether it is a Red Team attack or an actual assault, is to detect and respond to all security incidents. For this reason, the Blue Team is continuously on-call and must react to Red Team breaches the same way they would for any other adversary.

## Detection and Analysis

To detect malicious activity, Office 365 centrally logs security events and other telemetry and performs various analytical techniques to find anomalous or suspicious activity. Log files are collected from Office 365 servers and infrastructure devices and store them in a central and consolidated database.

As developing step-by-step processes for handling every potential incident is impossible, Microsoft takes a risk-based approach to detecting malicious activity. We leverage incident data and threat intelligence to define and prioritize our detections.

Employing a team of highly-experienced, proficient, and skilled people is one of the most important pillars to success in the detection and analysis phase. Office 365 employs multiple service teams, and those teams include employees with competencies on all components within the stack, including the network, routers and firewalls, load balancers, operating systems, and applications.

The security detection mechanisms in Office 365 also include notification and alerts that are initiated by different sources. The Office 365 Security Incident Response team is the key orchestrator of the security incident escalation process. This team receives all escalations and is responsible for analyzing and confirming the validity of the security incident.

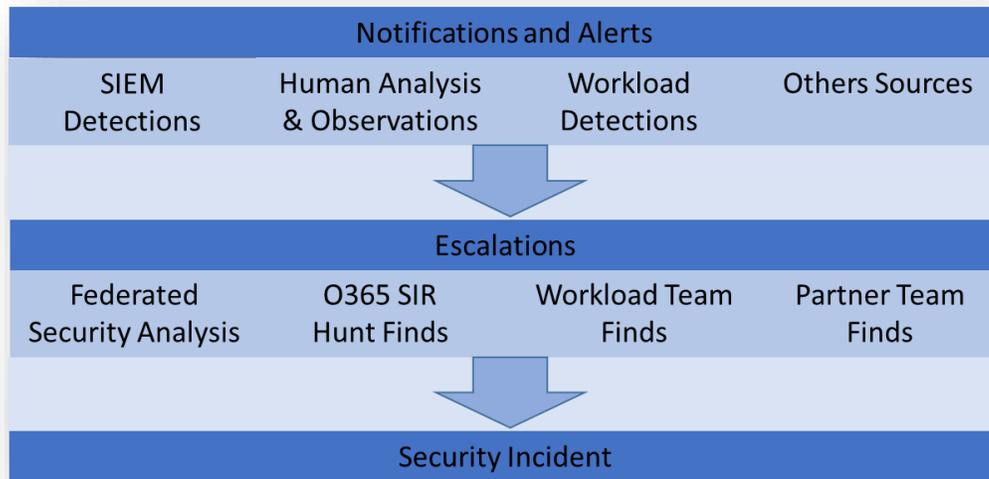


Figure 2 - Security Incident Management Process

One of the primary pillars of detection is notification:

- Each service team is responsible to log any action or event inside the service based on the recommendation from the Office 365 Security team. All logs created by the different service teams are processed by a Security Information and Event Management (SIEM) solution with predefined security and detection rules. These rules are evolving based on the Office 365 Security team's recommendation, and on information learned from previous security incidents, to determine if there is any suspicious or malicious activity.
- If customer determines that a security incident is underway, they may open a support case with Microsoft, which is assigned to the Office 365 CXP Communications team and turned into an escalation.

During the Escalation phase and depending on the nature of the security incident, the Office 365 Security Incident Response team may engage one or more subject matter experts from various Microsoft teams, such as the Online Services Security and Compliance team, MSTIC, MSRC, CELA, Azure Security, Office 365 engineering, and others.

Before any escalation to the Office 365 Security Incident Response team occurs, the service team is responsible for determining and setting the severity level of the security incident based on defined criteria such as privacy, impact, scope, number of affected tenants, region, service, details of the incident, and specific customer industry or market regulations.

Incident prioritization is determined by using distinct factors, including but not limited to the functional impact of the incident, the informational impact of the incident, and the recoverability from the incident.

After receiving an escalation about a security incident, the Office 365 Security team organizes a virtual team (v-team) comprised of members from Office 365 Security Incident Response team, service teams and the Office 365 Incident Communication team. The more complex part of activities of this v-team is to confirm the security incident and to eliminate any false positives. The accuracy of information provided by the indicators determined in the Preparation phase is critical. By analyzing this information by category of vector attack, the v-team can

determine if the security incident is a legitimate concern. At the beginning of the investigation, the Office Security Incident Response team records all information about the incident and updates during the incident lifecycle, which includes:

- A summary, which is a brief description of the incident and its potential impact
- The incident's severity and priority, which are derived by assessing the potential impact
- A list of all indicators identified which led to detection of the incident
- A list of any related incidents
- A list of all actions taken by the v-team
- Any gathered evidence, which will also be preserved for post-mortem analysis and future forensic investigations
- Recommended next steps and actions

The flow chart shown in Figure 3 details the Office 365 Security Incident Response team's process from the beginning of an escalation to containment, eradication, and remediation.

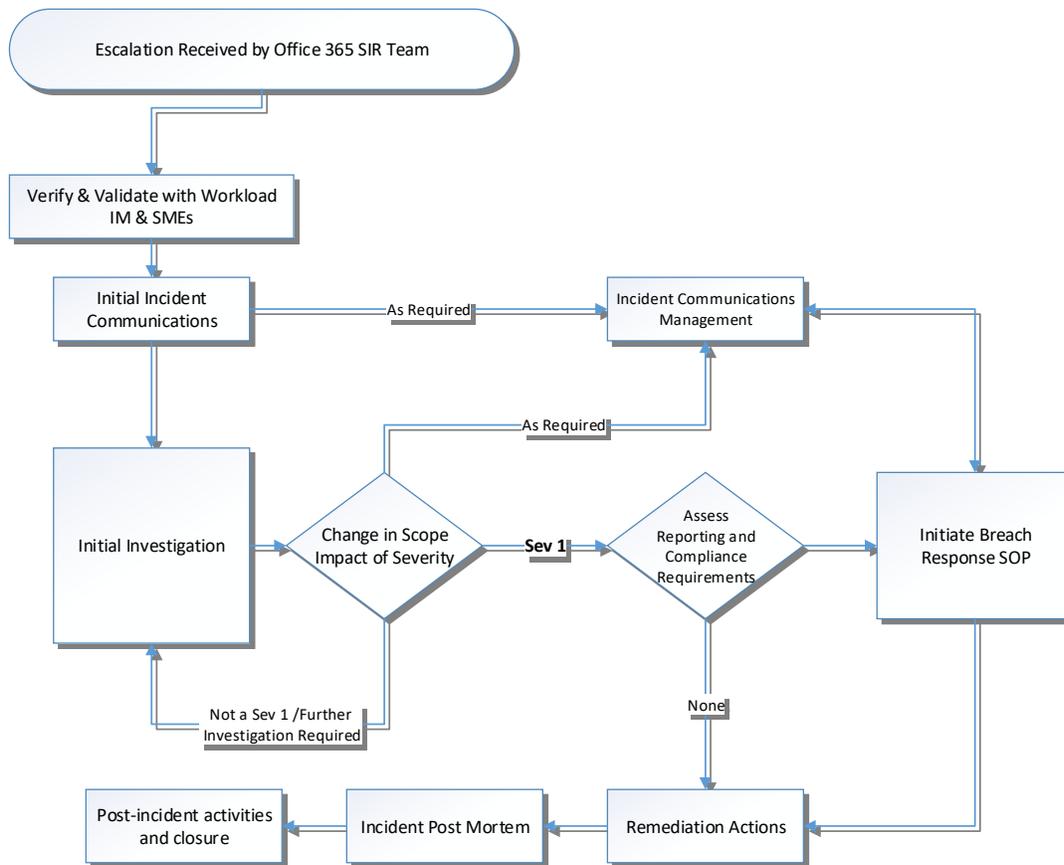


Figure 3 - Office 365 Security Investigation and Response Incident Flow

After security incident confirmation, the primary goals of the Office 365 Security Incident Response team and the appropriate service team are to contain the attack, to protect the service(s) under attack, and to avoid a greater global impact. At the same time, the appropriate engineering teams work to determine the root cause and to prepare the first remediation plan. In the next phase, the Office 365 Security Incident Response team identifies the customer(s) affected by the security incident, if any. The scope of effect can take some time to determine, based on region, datacenter, service, server farm, server, and so forth. The list of affected customers

is compiled by the service team and the Office 365 CXP Communications team, who then handle the customer notification process.

Office 365 service teams also use the intelligence gained in trend analysis through security monitoring and logging to detect abnormalities in Office 365 information systems that might indicate an attack or a security incident. Office 365 servers aggregate output from these logs in the production environment into a centralized logging server. From this centralized logging server, logs are examined to spot trends throughout the production environment. Data aggregated in the centralized server is securely transmitted into a logging service for advanced querying, dashboard building and detecting anomalous and malicious activity. The service also uses machine learning to detect anomalies with log output.

## Containment, Eradication and Remediation

Based on the analysis performed by the Office 365 Security Incident Response team, the service team, and others, an appropriate containment and remediation plan is developed to minimize the effect of the security incident. The appropriate service team(s) then applies that plan in production with support from the Office 365 Security Incident Response team.

Using Yammer as an example, after receipt of a security event, or on the detection of anomalous behavior in Yammer's production environment, a Yammer first responder triages the event, creates a ticket in Microsoft's internal issue tracking software and assigns it a priority. The responder also informs the MSRC about the case.

From this point, the First Responder(s) must classify the event in one of two buckets:

- **MSRC case** A publicly reported security issue is escalated to MSRC from the Yammer first responder. After escalation, a MSRC case number is assigned along with the appropriate severity, priority and likelihood. Yammer Security assesses and decides if the flaw is a known issue (is in the process of addressing or has been addressed) or if it is indeed a security vulnerability. Depending upon the severity, priority and likelihood of the case, Yammer Security and MSRC will decide on an appropriate fix timeline.
- **Software Security Incident Response Plan** A software security incident is defined as an elevated risk to customer data due to software vulnerabilities. The response plan is the MSRC's plan of action to react, assess and remedy these incidents.

YSO will also notify Microsoft executives and senior management during a software security incident and provide them with periodic updates. In addition, YSO will notify security contacts from Microsoft Online Risk Management when there is a possible instance of unauthorized access or unauthorized use resulting in the loss, disclosure, or alteration of customer data.

## Containment

After detecting a security incident, it is important to contain the intrusion before the adversary can access more resources or cause additional damage. Thus, the primary goal of our security incident response procedures is to limit impact to customers or their data, or to Microsoft systems, services and applications.

## Eradication

Eradication is the process of eliminating the root cause of the security incident with a high degree of confidence. The goal is two-fold: to evict the adversary completely from the environment and (if known) to mitigate the vulnerability that enabled or could enable the adversary to re-enter the environment. Depending on the nature of the incident, the scope of the security incident, the depth of the penetration and possible repercussions, the

Office 365 Security Incident Response team will recommend that service teams adopt eradication techniques. Considering the potential business impact that may be caused by these eradication steps, these decisions will be made by service teams and the Office 365 Security Incident Response team after a detailed analysis and approval from the Executive Incident Manager, if necessary.

## Recovery

As the response team gains reasonable level of confidence that the adversary has been evicted from the environment and all known vulnerable paths have been eliminated, the individual service teams, in consultation with the Office 365 Security Incident Response team, will initiate restoration steps to bring the service to a known and good configuration. This includes identifying the last known good state of the service, restoring from backups to this state, inspecting vulnerable attack paths in the restored state, etc. The Office 365 Security Incident Response team, in consultation with the service teams, will determine the best possible recovery plan for the environment.

A key aspect to the recovery is to have enhanced vigilance and controls in place to validate that the recovery plan has been successfully executed, and that no signs of breach exist in the environment.

## Notification of Security incident

If Microsoft determines that a security incident has occurred, we will notify you promptly. After identifying all affected tenants, the Office 365 CXP Communications team works to identify any relevant regulations that might apply to affected tenants. The Office 365 CXP Communications team uses the appropriate communication channel defined in applicable regulations to notify the appropriate tenant contact. Notification will include detailed information about the incident, such as a description of the incident, the effect on customer data, if any, actions taken by Microsoft, and/or suggested actions for customers to take to resolve the issue and prevent recurrence. Notification will be delivered to the designated administrator(s) of the Office 365 tenant. To ensure notifications are received, you should ensure that your administrators provide and maintain accurate contact information in their tenant profiles. In addition, depending on the nature of the incident, customers can also be notified via the Office 365 Service Health Dashboard, and via other service team portals, such as <http://status.yammer.com>.

## Post-Incident Activity

### Post mortem

After every security incident, the Office 365 Security Incident Response team conducts a detailed post-mortem with all the parties involved in security incident response to list out the sequence of events that caused the incident, and to create a technical summary of the incident as supported by the evidence that includes the actors involved in the breach (if known), how the response was executed, and other key takeaways. The post-mortem is designed to identify technical lapses, procedural failures, manual errors, process flaws and communication glitches, and/or any previously unknown attack vectors that were identified during the security incident response. The post-mortem will directly influence Office 365 service improvement, operational processes, and documentation by setting new priorities in the Office 365 engineering development cycle.

### Documentation

All key technical findings in the post-mortems are captured in a report as well as service investments or fixes in the form of bugs or development change requests. These are then followed-up with the appropriate engineering teams. In the case of process failures and cross-organizational issues, issues are documented in the

Office 365 Security Incident Response team's database and followed-up with the appropriate groups to address them.

## Process improvement

Responding to a security incident in Office 365 involves coordination with multiple groups spread across different organizations within Microsoft, and potentially even appropriate external organizations such as law enforcement. We know that it is critical to evaluate our responses after every security incident for both sufficiency and completeness. In case of any identified improvements or changes, the Office 365 Security Incident Response team evaluates the suggestions in consultation with the appropriate teams and stakeholders, and where appropriate incorporates them into standard operating procedures. All required changes, bugs or service improvements identified during the security incident response or post-mortem activity are logged and tracked in an internal Office 365 engineering database, and all potential bugs or features are assigned to the appropriate owner. The Office 365 Security Incident Response team reviews all entries until the issue is resolved.

## Summary

Microsoft works continuously to provide highly secure, enterprise-grade services for Office 365 customers. Our process for managing a security incident conforms to the approach prescribed in NIST 800-61, and we have several dedicated teams that work together to prevent, monitor, detect, and respond to security incidents. The Office 365 Security team and the service teams work jointly and take the same approach to security incidents, which include Preparation; Detection and Analysis; Containment, Eradication, and Remediation; and Post-Incident Activity.

## Materials in this Library

Microsoft publishes a variety of content for customers, partners, auditors, and regulators around security, compliance, privacy, and related areas. Below are links to other content in the Office 365 CXP Risk Assurance Documentation library.

Name	Abstract
<a href="#">Auditing and Reporting in Office 365</a>	Describes the auditing and reporting features in Office 365 and Azure Active Directory available to customers. Also details the various audit data that is available to customers via the Office 365 Security & Compliance Center, remote PowerShell, and the Management Activity API. Also describes the internal logging data that is available to Microsoft Office 365 engineers for detection, analysis, and troubleshooting.
<a href="#">Controlling Access to Office 365 and Protecting Content on Devices</a>	Describes the Conditional Access (CA) features in Microsoft Office 365 and Microsoft Enterprise Mobility + Security, and how they are designed with built-in data security and protection to keep company data safe, while empowering users to be productive on the devices they love. It also provides guidance on how to address common concerns around data access and data protection using Office 365 features.
<a href="#">Data Encryption Technologies in Office 365</a>	Provides an overview of the various encryption technologies that are used throughout Office 365, including features deployed and managed by Microsoft and features managed by customers.
<a href="#">Data Resiliency in Office 365</a>	Describes how Microsoft prevents customer data from becoming lost or corrupt in Exchange Online, SharePoint Online, and Skype for Business, and how Office 365 protects customer data from malware and ransomware.
<a href="#">Defending Office 365 Against Denial of Service Attacks</a>	Discusses different types of Denial of Service attacks and how Microsoft defends Office 365, Azure, and their networks against attacks.
<a href="#">Financial Services Compliance in Microsoft's Cloud Services</a>	Describes how the core contract amendments and the Microsoft Regulatory Compliance Program work together to support financial services customers in meeting their regulatory obligations as they relate to the use of cloud services.
<a href="#">Microsoft Response to New FISC Guidelines in Japan (English) (Japanese)</a>	Explains how Microsoft addresses the risks and requirements described in the FISC Revised Guidelines, and it describes features, controls, and contractual commitments that customers can use to meet the requirements in the Revised Guidelines.
<a href="#">Microsoft Threat, Vulnerability, and Risk Assessment of Datacenter Physical Security</a>	Provides an overview regarding the risk assessment of Microsoft datacenters, including potential threats, controls and processes to mitigate threats, and indicated residual risks.
<a href="#">Office 365 Administrative Access Controls</a>	Provides details on Microsoft's approach to administrative access and the controls that are in place to safeguard the services and processes in Office 365. For purposes of this document, Office 365 services include Exchange Online, Exchange Online Protection, SharePoint Online, and Skype for Business. Additional information about some Yammer Enterprise access controls is also included in this document.
<a href="#">Office 365 Customer Security Considerations</a>	Provides organizations with quick access to the security and compliance features in Office 365 and considerations for using them.
<a href="#">Office 365 End of Year Security Report 2014</a>	Covers security and legal enhancements made to Office 365 in calendar year 2014 that enables customers and partners to meet legal requirements surrounding independent verification and audits of Office 365.
<a href="#">Office 365 End of Year Security Report and Pen Test Summary 2015</a>	Office 365 End of Year Security Report and Pen Test Summary for CY 2015.
<a href="#">Office 365 Mapping of CSA Cloud Control Matrix 3.0.1</a>	Provides a detailed overview of how Office 365 maps to the security, privacy, compliance, and risk management controls defined in version 3.0.1-11-24-2015 of the Cloud Security Alliance's Cloud Control Matrix.
<a href="#">Office 365 Risk Management Lifecycle</a>	Provides an overview of how Office 365 identifies, evaluates, and manages identified risks.
<a href="#">Privacy in Office 365</a>	Describes Microsoft's privacy principles and internal standards that guide the collection and use of customer information at Microsoft and give employees a clear framework to help ensure that we manage data responsibly.
<a href="#">Self-Service Handling of Data Spills in Office 365 (restricted to Federal customers)</a>	Reviews the spillage support provided by Office 365, the tools available to customers, and the configuration settings that should be reviewed in environments that are prone to data spills.
<a href="#">Tenant Isolation in Office 365</a>	Describes how Microsoft implements logical isolation of tenant data within Office 365 environment.