Genpact Information Security – Incident Response Plan

Version – 3.2

Transformation Happens Here

Table of Contents

Introduction 6

Purpose 6

Scope 6

Genpact Incident Response Team's Roles & Responsibilities 8

Incident Response – Framework 9

Preparation 10

Detection and Analysis 10

Analysis 12

Prioritisation of Incidents 12

Incident Response Workflow 14

Containment, Eradication and Recovery 15

Containment 15

Eradication 15

Recovery 16

Notification and Communication 16

Post Incident Activities 18

Documentation 18

Root Cause Analysis 19

Lessons Learned 19

Management of Evidence 19

Genpact Risk Council 20

Handling of Ransomware Incidents 20

Incident Response Plan Maintenance 21

Incident Response Plan Testing 21

Incident Metrics 21

Incident Review Process 22

Escalation matrix is maintained at the below SharePoint location 22

Communication matrix is maintained at the below SharePoint location 22

Appendix A: GENPACT Privacy Incident & Breach Response Plan 22

Document Revision History

Version No.	Version Date	Type of changes	Author	Approver	Date of Next Review
1.0	03 Feb,2003	Initial	Akhil Manchanda		
1.1	13th Oct, 2003	Contact details updated, Common procedures added	Akhil Manchanda		
1.1.1	18th Jul, 2005	Contact details updated	A R Vijay		
1.2	7th Aug, 2006	Contact details updated	A R Vijay		
1.3	7th Dec, 2006	Contact details updated	A R Vijay		
1.4	23rd May' 2007	Contact details updated	Infosec team		
1.5	3rd Jun, 2008	Contact details updated, Global teams included	Infosec team		
1.6	15th Dec'08	SMG lead, ISL-US detail updated, Detection of wireless rogue device is added in Appendices F, Appendices H added	Infosec/ Vikas		2nd Jun'09
1.7	1st May'09	Contact details updated	Infosec/ Vikas		1st May'10
1.8	26th Oct'09	Contact details updated (Network Lead & EU ISL)	Infosec/ Vikas		Need based
1.9	18th Jan '10	Contact details updated	Infosec/ Sekhar		Need based
1.10	8th Apr '10	Contact details updated	Infosec/ Sekhar		Need based
1.11	17th Sep 10	Contact details Updated	Infosec/ Sekhar		Need based

1.12	31st Jan 2011	Contact details Updated	Infosec/ Sekhar		Need based
1.13	10th Feb 2012	Included Incident response test slide	InfoSec/Satish Jagu		Need based
1.14	18th Apr 2012	Included RACI and Communication plan	InfoSec/Satish Jagu		18th Apr 2013
1.15	30th May 2012	Review and changes as per internal discussion	InfoSec/Satish Jagu		30th May 2013
1.16	22nd Feb 2013	Contact details Updated	InfoSec/Sekhar		Need based
1.17	20th July 2013	Contact details, identification and links Updated	InfoSec/Sekhar		Need based
1.18	13th Mar 2014	Contact details Updated	InfoSec/Sekhar		Need based
1.19	23rd Mar 2015	Added Annexure and updated contact details	Ankur Jain		Need based
1.20	21st Apr 2016	Contact Details Updated	Satish Jagu	Ramachandra Hegde	Need Basis
2.0	21 Jun 2016	Document changed to – Incident Response Plan	Satish Jagu	Ramachandra Hegde	20 Jun 2017
2.1	23 Feb 2017	Included Genpact Data Privacy document	Satish Jagu	Ramachandra Hegde	22 Feb 2018
2.2	8 Sep 2017	Included details of Contact number of CDC, Retention of Evidence duration,	Satish Jagu	Ramachandra Hegde	7 Sep 2018
2.3	11 July 2018	Updated risk rating criteria and communication plan	Uday Bose	Ramachandra Hegde	10th July 2019
3.0	21st February 2019	Alignment of Genpact Privacy Incident & Breach Response Plan	Uday Bose	Ramachandra Hegde	20th February 2020

3.1	21st February 2020	Updated definition: Preparation, Identification, Analysis and Security Incident Replaced Detection Time by Actual Occurrence Time in the Containment Time metric.	Uday Bose	Ramachandra Hegde	20th February 2021
3.2	21st February 2021	**Updates:** Definition - Event, Security Incident, Vulnerability, Threat Incident Response Steps, Roles and Responsibilities, Detection technologies and monitoring coverage, Incident workflow - Incident declaration criteria, Incident Communication Plan, Post Incident Activities Replaced Actual Occurrence Time with Investigation Start Time for Containment Time metric. **New Inclusions:** Scope, Genpact Risk Council, Ransomware Incident Handling Process, Incident Review Process	Uday Bose	Ramachandra Hegde	21 February 2022

Introduction

In an environment of increasingly sophisticated threats, complex and increasingly stringent compliance and client requirements, it is imperative for Genpact to ensure it has a world class information security program. Genpact has thus adopted a “defence in depth” strategy.

A critical element of this strategy is having a strong detection and response capability to build cybersecurity resilience. This strategy recognizes that while preventive controls are important, vulnerabilities/threats are often unknown in the larger ecosystem, there is an increased reliance on third parties and the threat actors are sophisticated thus these preventive controls while necessary are insufficient and detective and response procedures are equally, if not more critical. Thus, the security program must have strong capabilities to maintain situational awareness and to rapidly detect and effectively respond to a broad range of incident scenarios.

Purpose

The purpose of the Incident Response Plan is to mitigate the risks arising out of security incidents by providing guidance on responding to incidents effectively and efficiently. The primary focus of the document is detection, analysis, prioritization, and handling of security incidents. It has been established to take measures to protect Genpact Global IT environment, develop and publish response procedures and disseminate documentation and best practice recommendations to employees.

The goals of the incident response team include:

- Detect and Respond to information security incidents.
- Contain the impact of the incident.
- Maintain and/or restore business continuity in case of an information security incident.
- Determine the root cause of the incident occurrence.
- Ensure existing policies and standards are followed and updated to prevent further attack.
- Preserve evidence.
- Keep Leadership informed of the situation and response.

Scope

This plan is applicable to all the security incidents which includes Genpact employees, Contractors and Third-Party Vendor personnel having access to Genpact Information and Information Systems plan and to all regions, countries, business units, sites, and functions that operate within Genpact.

Definitions

To establish the scope of response efforts and create a foundation for consistency in the categorization, communication, and handling of security-related event and alert, incident occurrences will be categorized as an event, alert, or an incident.

Event – Any observable occurrence in an application, system, or network, which may originate on an individual system, a network, a security device, any other device, or applications.

Events can be detected in a wide variety of ways by any number of different sources. An event may indicate that the security of an information system, service, application, or network has been affected or altered. An event may also indicate that an information security policy may have been violated, or that a safeguard might have failed.

Examples of **Events** include **but** not limited to the below:

- User accessing a file
- User Login
- Server receiving a request for a web page
- User sending electronic mail (e-mail)
- Firewall blocking an incoming/outgoing connection
- Execution of a command or launch of an application
- Modification of the system registry
- Unexpected or malformed network packets
- Firewall configuration changes

Alert - An alert is an outcome of correlation of different events to identify deviations from normal behaviour or violation of security policies which can be a potential security incident.

Examples of an **Alert** include**,** but not limited to the below**:**

- User downloading bulk files
- Multiple failed login attempts
- User sending email to a personal email address
- Malware infections
- Multiple location changes in quick succession
- Data uploaded on a public shared website
- Firewall blocking multiple connection attempts
- Communication to/from blacklisted IP addresses
- Multiple users deleted in short span of time
- High volume of operations in a key vault
- Change activity detected on built in admin account

Incident - A security incident is a violation or imminent threat of violation, which the organization has a factual basis for believing that a specific incident is about to occur or has already occurred. The violation can be a non-conformity of organizations Information Security Policy, Data Privacy Policy, Acceptable Usage Policy, or deviation of any standard security practices. The mentioned contravention can arise out of an alert, review, or some other mechanism.

Examples of an incident include, but not limited to below:

- An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.
- Users are tricked into opening a 'quarterly report' sent via email that is malware; running the tool infects their computers and establishes connections with an external host.
- An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money or alter a business practice.

- A user provides or exposes sensitive information, including personal information or sensitive personal information, to unauthorized recipients, through peer-to-peer file sharing services/email or web uploads, or other mechanisms.

Incidents often result in negative consequences to the organization, such as:

- System crashes
- Unauthorized use of system privileges
- Unauthorized access to sensitive data, including personal information or sensitive personal information
- Execution of malware that destroys data
- Data Leakage
- Asset theft/loss
- Brand Reputation/Financial Impact

Vulnerability: A vulnerability is a weakness, which can be exploited by a malicious actor to gain unauthorized access to or perform unauthorized actions on a computer system. Vulnerabilities can allow malicious actors to run a code, access a system's memory, install malware, and steal/destroy or modify sensitive data.

Examples of common vulnerabilities includes, but not limited to the below:

- OS command injection
- SQL injection
- Buffer overflow
- Missing authentication for critical function
- Missing authorization
- Unrestricted upload of dangerous file types
- Reliance on untrusted inputs in a security decision

Threat: A threat is a potential negative action or event facilitated by a vulnerability that results in an unwanted impact to a computer system/application/network. A threat can be either a negative "intentional" event (i.e. hacking: an individual cracker or a criminal organization) or an "accidental" negative event (e.g. the possibility of a computer malfunctioning, or the possibility of a natural disaster event such as an earthquake, a fire, or a tornado) or otherwise a circumstance, capability, action, or event.

Following are the examples of common threats, but not limited to:

- Unauthorized access
- Computer viruses
- Asset/Data theft/Sabotage
- Vandalism/Accidents

Genpact Incident Response Team’s Roles & Responsibilities

Genpact’s **Chief Information Security Officer** has formed an Incident Response Team within the information security function and have appointed an Incident Response Leader. This team acts as the primary team for handling all types of security incidents. The Incident Response Team is responsible for managing the end to end life cycle of a security incident. In case of any security incident, the Incident Response Team opens and maintain lines of communication with affected constituents during the incident handling process.

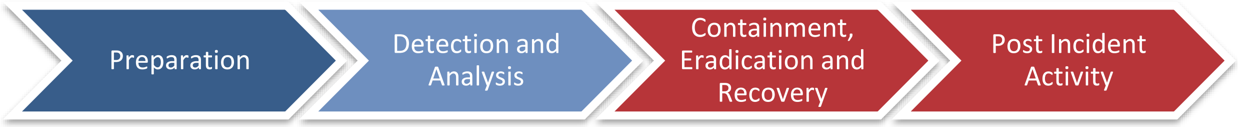
Based on the nature of the incident and potential consequences, a broader Incident Response Team is developed with appropriate representation from other functions and stakeholders including IT, Data Privacy, Legal, Human Resource, Communications (media/social media/internal comms/regional comms), Investor Relations, Physical Security, Risk and Compliance etc.

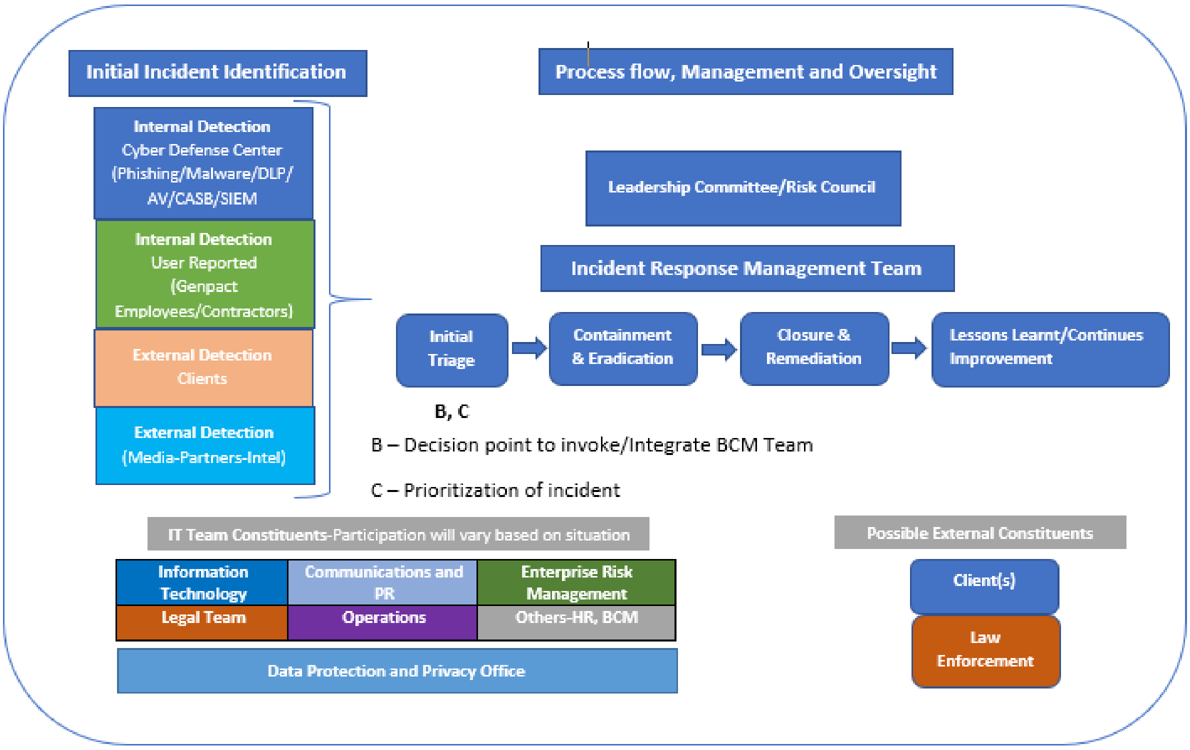
The table below lists the key participants in the Incident Response Team. The Incident Response Team constitutes of incident response leader, supporting analysts, and other participants from within and outside the organization, as needed:

Incident Response Team	**Incident Response Leader:** Coordinate response efforts and serve as the main point of contact.
	Incident Response Analysts: Execute containment, eradication, and recovery steps.
	Forensic Investigators: Collect and analyze evidence from the incident.
Subject Matter Experts	**Information Security:** Provide subject matter expertise.
	Information Technology: Manage IT infrastructure, network, and application fixes as part of response.
	Data Protection and Privacy Office: Subject matter expertise for privacy related incidents.
Other Corporate Functions	**Communications:** Notify customers, media, and third parties.
	Corporate Security: Conduct criminal and fraud investigations and liaise with law enforcement.
	Human Resources: Investigate corporate policy violations.
	Legal: Provide legal guidance. Identify and file required regulatory submissions.
	Physical Security: Deal with loss of physical systems or aid in confiscation of media.
	Enterprise Risk Management: Assess non-compliance to operational policies and procedures, as well as client provided compliance requirements
	Affected Business Unit Management: Provide business perspective and buy-in for response actions. Coordinate outreach involving customers
	Audit: Provide expertise in compliance-related incidents. Investigate suspicions of internal fraud and abuse.
	Business Continuity: Assist with system outages caused by the incident or by recovery actions.
	Other Required Members
	As-Needed Team Members
External Partners	Incident Response Retainer
	Managed Detection and Threat Hunting

Incident Response – Framework

Event, Alert, and Incident management is an important component of an information security program. Our methodology is designed to minimize business impact, return computing services to normal operations, reduce risk of data loss, and enable compliance to applicable regulations and standards. The overall approach to Incident Response has been modeled on the NIST framework as outlined below:




Initial Incident Identification
Internal Detection Cyber Defense Center (Phishing/Malware/DLP/ AV/CASB/SIEM
Internal Detection User Reported (Genpact Employees/Contractors)
External Detection Clients
External Detection (Media-Partners-Intel)
Process flow, Management and Oversight
Leadership Committee/Risk Council
Incident Response Management Team
Initial Triage
Containment & Eradication
Closure & Remediation
Lessons Learnt/Continues Improvement
B, C
B – Decision point to invoke/Integrate BCM Team
C – Prioritization of incident
IT Team Constituents-Participation will vary based on situation
Information Technology
Communications and PR
Enterprise Risk Management
Legal Team
Operations
Others-HR, BCM
Data Protection and Privacy Office
Possible External Constituents
Client(s)
Law Enforcement

Preparation

The Preparation section of Genpact Incident Response Plan establishes a link with the incident detection processes and defines criteria to categorize incidents. Incident Response methodologies emphasize preparation phase – not only from establishing an incident response capability, but also preventing the incidents by ensuring that network, systems, and applications are sufficiently secured. Genpact Incident Response plan includes but not limited to the following activities as a part of the preparation phase

- 24x7 Host and Network monitoring
- Information Protection Program
- Endpoint protection and detection
- Patch Management
- Vulnerability Assessment/Penetration Testing
- Compliance and Security Awareness Training
- Review and Test Incident Response Procedures
- Risk Assessments

Detection and Analysis

Incidents can occur in countless ways and from different incident sources. So, effective ways for both internal and external parties to report incidents is equally critical. Genpact Incident Response Plan is a generic approach designed to cater different types of incidents arising out of multiple incident detection channels.

Incident Detection Channels

	Internal Sources	External Sources
Active Detection	SIEM-Qradar	Managed Security Service Provider (MSSP)
	Cofense	
	Azure Sentinal	
	Digital Shadows	
	CrowdStrike	
	Anti-Virus	
	Symantec DLP	
	Symantec CASB/Microsoft MCAS	
	Prisma Cloud	
	Threat Intelligence	
	Observe IT	
Passive Detection	Notification by Genpact Employees and Contractors	Threat Intel/Client/Vendor notification

Technology	Monitoring coverage
IBM Qradar and Azure Sentinel	Logs correlation, User behavior analytics (UBA), Threat Feeds.
Digital Shadows	Brand reputation/impersonation monitoring, data leakage on public websites, dark web monitoring, threat intelligence, attack surface monitoring.
Cofense	Suspicious emails reported by employees.
Observe IT	Insider threat monitoring.
Threat intelligence	Cyber threat advisories.
Prisma Cloud	Cloud configuration and cloud flows monitoring.
CrowdStrike	Endpoint detection and response (EDR)
Symantec DLP	Data leakage prevention and detection
Microsoft CASB/MCAS	Monitoring of cloud applications usage via CASB (Cloud application security broker)
Multiple technologies	Threat hunting and Analytics

Channels to notify

Entity	Notification
Genpact Employees/Contractors	InfoSec@genpact.com
Genpact Clients/External Agencies	CSIRT@genpact.com

Analysis

Once a potential incident has been identified, the Incident Response Team will be activated to investigate the situation. The assessment will determine the incident category, scope, and potential impact of the incident. The Incident Response Team shall quickly analyse and validate the incident and perform the necessary steps including but not limited to as mentioned below. These actions may vary based on the incident scenarios.

- Initial Triage
- Identify affected data/systems
- Gather information and data
- Assessment of Risk
- Identification of PII/SPI/Other regulatory elements

Prioritisation of Incidents

Security Incidents should be prioritized based on the risk rating of the incident as prioritizing the incidents is the most critical decision point in the incident handling process

Risk rating of an incident should be calculated based on the impact of the incidents and following factors will contribute to determine the risk rating of an incident.

- Loss of Confidentiality, Integrity and Availability
- Financial and Brand Reputation Damage
- Regulatory Impact

Impact on all these factors will be assessed for each incident as per below scale

Loss of Confidentiality – Current or Potential	
No data/Public data disclosed	1
Genpact internal/ Client equivalent data disclosed	2
Genpact confidential/ Client equivalent data disclosed	3
Genpact restricted/Client equivalent data disclosed	4

Loss of Integrity – Current or Potential	
No data/Public data altered or changed	1
Genpact internal/ Client equivalent data altered or changed	2
Genpact confidential/ Client equivalent data altered or changed	3
Genpact restricted/Client equivalent data altered or changed	4

Loss of Availability – Current or Potential	
All Data and Services are available to users/client	1
Minimal effect, the organization can still provide all critical services to all users/client but has lost efficiency	2
Organization has lost the ability to provide a critical service to a subset of system users/client	3
Organization is no longer able to provide some critical services to any users/client	4

Financial Damage – Current or Potential	
No financial damage/Minimal impact<1000 USD	1
Minor impact <100K	2
Major impact >100K <1M	3
Significant impact >1M	4

Brand Reputation Damage – Current or Potential	
No brand reputation impacted	1
Minor Impact [Brand reputation with single client impacted]	2
Major Impact [Brand reputation with multiple clients impacted]	3
Significant Impact [Print and Electronic Media]	4

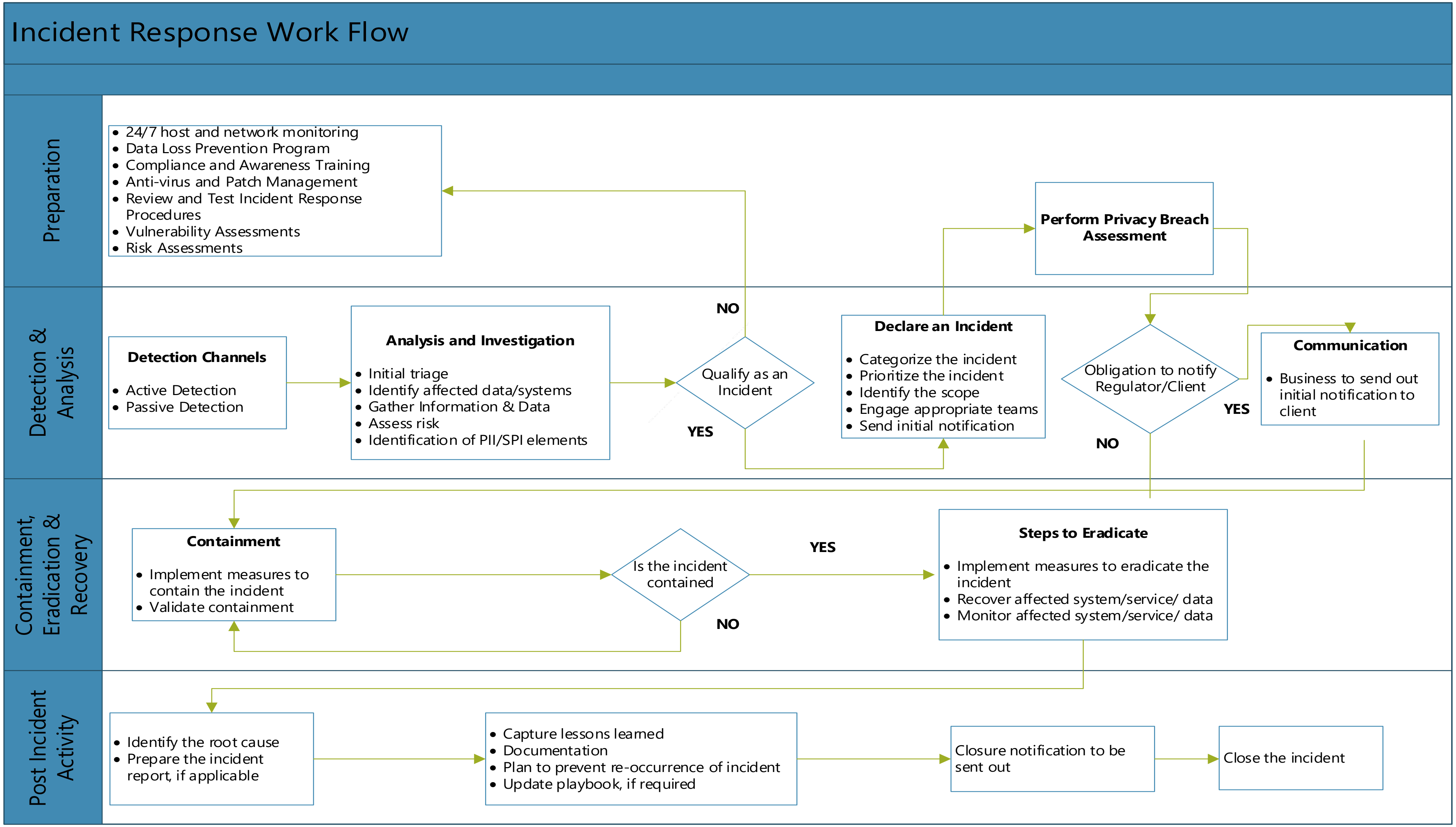
Regulatory Impact – Current or Potential	
No regulatory impact	1
Any regulatory impact with notification deadline (within 30 days) of incident detection	2
Any regulatory impact with notification deadline (within 15 days) of incident detection	3
Any regulatory impact with stringent timeline (within 72 hours) of incident detection	4

The final risk score of an incident will be based on the addition of above factors/parameters and will be categorized as per below mentioned risk scale:

Critical 18-24	Disastrous situation when organization's business operation is severely affected.
High 13-17	Significant level of impact resulting in disruption of services to a section of business operations.
Medium 8-12	Moderate level of impact causing no obstruction on the business operations.
Low 6-7	Little or no impact on any aspect of the business operation.

Incident Response Workflow

The below flowchart illustrates the Incident Response process utilized at Genpact.



Incident Response Work Flow

Preparation

- 24/7 host and network monitoring
- Data Loss Prevention Program
- Compliance and Awareness Training
- Anti-virus and Patch Management
- Review and Test Incident Response Procedures
- Vulnerability Assessments
- Risk Assessments

Perform Privacy Breach Assessment

Detection & Analysis

Detection Channels

- Active Detection
- Passive Detection

Analysis and Investigation

- Initial triage
- Identify affected data/systems
- Gather Information & Data
- Assess risk
- Identification of PII/SPI elements

Qualify as an Incident

NO

YES

Declare an Incident

- Categorize the incident
- Prioritize the incident
- Identify the scope
- Engage appropriate teams
- Send initial notification

Obligation to notify Regulator/Client

YES

NO

Communication

- Business to send out initial notification to client

Containment, Eradication & Recovery

Containment

- Implement measures to contain the incident
- Validate containment

Is the incident contained

YES

NO

Steps to Eradicate

- Implement measures to eradicate the incident
- Recover affected system/service/ data
- Monitor affected system/service/ data

Post Incident Activity

- Identify the root cause
- Prepare the incident report, if applicable

- Capture lessons learned
- Documentation
- Plan to prevent re-occurrence of incident
- Update playbook, if required

Closure notification to be sent out

Close the incident

Containment, Eradication and Recovery

Containment

Containment of the incident is necessary to minimize and isolate the damage caused. Steps shall be taken to ensure that the scope of the incident does not spread to include other systems and Information Resources. Examples of containment actions are mentioned below, but not limited to:

Phase	Type	Containment Actions
Containment	Stolen Credentials	Disable account credentials, reset all active connections, review user activity, reverse changes, increase alerting, harden from future attacks.
	Ransomware	isolate the impacted system, validate the ransomware claim, contact insurance carrier, identify whether additional systems have been impacted and isolate as needed.
	Virus Outbreak	Contain LAN/System
	Data Loss	Review User Activity, Implement Data Breach response procedures.

Containment requires critical decision-making related to the nature of the incident. The Incident Response Team along with other members of the incident investigation team should review all the containment steps to formulate a strategy to contain and limit damages resulting from the incident and gather evidences as deemed necessary. Depending on the type of incident, team should clearly outline the scope of the incident and act appropriately to reduce the impact to affected systems and/or reduce the reach to other systems. Actions may include, but are not limited to the following:

- Stop the attacker using access controls (disabling accounts, resetting active connections, changing passwords, implementing router ACLs or firewall rules, etc.).
- Isolate compromised systems from the network.
- Avoid changing volatile state data or system state data early on.
- Identify critical external systems that shall remain operational (e.g. email, client application, DNS) and deny all other activity.
- Maintain a low profile, if possible, to avoid alerting an attacker that you are aware of their presence.
- Permanent deletion of the emails/documents/data from the unintended recipient's mailbox and capture the evidences to the extent possible.

Eradication

Eradication requires removal or addressing of all components and symptoms of the incident. Further, validation shall be performed to ensure the incident does not reoccur. Steps to eradicate components of the incident may include:

- Disable compromised user accounts.
- Reset any active sessions for compromised accounts.
- Identify and mitigate vulnerabilities leveraged by the attacker.

- Close unnecessary open ports.
- Increase authentication security measures (implement MFA, add geolocation restrictions).
- Increase security logging, alerting, and monitoring.

Recovery

Recovery involves the steps required to restore data and systems to a healthy working state allowing business operations to be returned. Prior to restoring systems to normal operation, it is essential that the incident management team validate the system(s) to determine that eradication was successful, and the network/system is secure.

Recovery steps may include the below actions, but not limited to:

- Restoring systems from a clean backup.
- Replacing corrupted data from a clean backup.
- Restoring network connections and access rules.
- Engaging a third party for support in detecting or preventing future attacks.

Notification and Communication

Effective communication during an incident response, and throughout the life cycle of an incident, is key to developing and sustaining an effective incident response program. Required notification and communication both internally and with third parties (customers, vendors, law enforcement, etc.) based on legal, regulatory, and contractual requirements should take place in a timely manner. The Incident Response Team should report the incident to the senior leadership (based on the risk rating/criticality).

Below table illustrates the communication plan for incidents based on risk ratings.

Category	Critical
Initial Notification – Duration	2 hours from the time Incident is detected
Initial Notification - Mode of Communication	Email notification/Bridge call
Internal Parties	IT Leadership, Business Leadership, Risk & Compliance, Data Privacy and Protection Office (as applicable)
External Parties	Client Point of Contact (If Impacted)
Incident Status Updates - Duration	Every 4 hours or as per conference call
Incident Status Updates	E-mail or Conference call
Category	**High**
Initial Notification – Duration	4 hours from the time Incident is detected

Initial Notification - Mode of Communication	Email Notification
Internal Parties	IT Leadership, Business Leadership, Risk & Compliance, Data Privacy and Protection Office (as applicable)
External Parties	Client Point of Contact (If Impacted)
Incident Status Updates - Duration	Weekly/Review Call
Incident Status Updates	E-mail

Category	Medium
Initial Notification – Duration	Notified on need basis
Initial Notification - Mode of Communication	Email Notification
Internal Parties	Incident Response Team members
External Parties	Client Point of Contact (If Impacted)
Incident Status Updates - Duration	Initial and Closure Notification
Incident Status Updates	E-mail

Category	Low
Initial Notification – Duration	Notified on need basis
Initial Notification - Mode of Communication	Email Notification
Internal Parties	Incident Response Team members
External Parties	Client Point of Contact (If Impacted)
Incident Status Updates - Duration	Initial and Closure Notification
Incident Status Updates	E-mail

Communication plan and timelines for other external stakeholders such as Regulators and Data Subjects (in case of privacy incidents) will be governed by applicable laws and regulations. ***Refer Appendix A***

Client who are affected by the incident should be notified according to applicable contract language, service level agreements or applicable statutes and/or regulations.

Post Incident Activities

Documentation

All details related to the incident response process should be formally documented and filed for easy reference. Whenever possible, the following items should be maintained:

- Identify affected systems/devices/accounts.
- Impact Analysis.
- Incident Artefacts validation.
- Analyse the incident.
- Remediation Actions Performed
- Resolution Summary/Resolution Action
- All external/internal communications
- Investigator Notes compiled

An incident report shall be prepared by the incident response team at the end of the incident management process. The report shall be approved by the Incident Response Lead along with Legal and Compliance team on required basis. The incident report will be prepared for High/Critical incident or if specifically asked by client or wherever applicable.

The below table provides a list of actions that shall be performed by Incident Response team depending upon the nature of the incident and additional steps may be included as deemed necessary.

General Guidelines for Incident Response	
Remain calm. Resist the tendency to overreact or panic. Methodically follow security policy.	
Assemble the team by sending a meeting notice to the Incident Response Team distribution list in email and use the call-in number.	
Objective 1 – Analysis and Investigation	
	Initial Triage
	Gather information/Review Logs
	Prioritize the incident with appropriate Risk Rating.
	Perform a Privacy Breach Assessment
	Engage appropriate teams for incident handling
Objective 2 – Communicate the Incident	
	Assemble and disseminate all relevant information.
	Compile all notes into a comprehensive security incident activity log.
	Distribute to incident participants for review and approval.
	Perform the root cause analysis and implement corrective measures to avoid future occurrences.
	Prepare incident report to management/client to explain as how the incident occurred, immediate steps taken, key findings from the investigation and how it will be prevented in the future.
Objective 3 – Contain the Damage and Minimize Risk	

	Act quickly to minimize the effect of the incident.
	Identify the resources that have been compromised.
	Disconnect compromised resources from the network and determine access points.
	Recover systems.
	Reevaluate and, if necessary, reassign risk rating to the incident.
Objective 4 – Review Response and Update Policies	
	Once the environment is protected, reassemble the team for a postmortem discussion.
	What steps were executed successfully?
	What mistakes were made?
	How can we improve processes to avoid a similar incident in the future?

Root Cause Analysis

Root cause analysis (RCA) is a method of problem-solving used to investigate known problems and identify their antecedent and underlying causes. While the term root cause analysis seems to imply that issues have a singular cause, this is not always the cause. Problems may have a singular cause, or multiple causes stemming from deficiencies in products, people, processes, or other factors.

Genpact Incident Response Team shall perform steps to establish the root cause for all incidents. IR Team should document the findings for High and Critical risk rated incidents or if specifically mentioned by business/client. Following steps may be performed to conclude the root cause of a security incident:

- Interviews with witnesses and/or affected persons.
- Capturing images, snapshots, or memory dumps of affected systems.
- Obtaining relevant documents.
- Conducting observations.
- Reviewing security camera footage.
- Analysing the logs of the various devices, technologies and hosts involved (e.g. firewall, router, anti-virus, intrusion detection, host).
- Reviewing email rules (compromised email account).
- Compare the compromised system to a known good copy.
- Anomaly detection/behaviour monitoring (compare to preestablished baseline).

Lessons Learned

The Lessons Learned phase includes post-incident analysis on the resources that were impacted by the incident and other potentially vulnerable resources. Lessons learned from the incident are communicated to executive management and action plans developed to improve future incident management practices and reduce risk exposure. An important aspect here to capture the lessons learned and update the existing playbooks and Standard Operating Procedures.

Management of Evidence

Evidence collection and maintenance of chain of custody (attached Appendix B) is also a crucial part of Incident Response. Tracking of forensic information collected while responding to incidents that may be useful in identifying adversaries, coordinating with law enforcement, and facilitating other investigative activity is stored in the Incident Management Tool (IBM Resilient). Various other sources of incidents and the location to store the incidents & relevant evidence is described in below:

Technologies	Storage Location
SIEM	QRadar Console
IDS/IPS	IDS/IPS and QRadar Console
Antivirus	Antivirus Console
DLP	Symantec DLP Console
Activity Logs (operating system, application, network, database, etc.)	On local Server and QRadar Console
Managed security services provider	MSS Console and cdc@genpact.com mailbox
IT help desk	Helpmate Portal and cdc@genpact.com mailbox
Infosec@genpact.com	Infosec@genpact.com
Vendor/service provider notification	csirt@genpact.com
Client Notification	csirt@genpact.com

Genpact Risk Council

The Genpact RC approves risk management related guidelines and policy and ensures that risk management system is established, implemented, and maintained in accordance with the defined framework. The RC meets quarterly to review risks and approves the organization's risk profile periodically.

The RC provides a sign off on the current & planned approach to manage key business risks and approves the risk mitigation plan and strategy ensuing it's in line with the company's risk appetite.

Handling of Ransomware Incidents

In the event that the company is a victim of a cyber extortion threat ("ransomware"), at the "engage appropriate teams" stage of the Incident Response Work Flow or as soon as practicable after the ransomware demand is received, the Chief Information Security Officer will inform the Genpact Risk Council of the information that is known at that time. The Genpact Risk Council will determine whether notification of the Audit Committee of the Board of Directors ("Audit Committee") is warranted. In parallel, as soon as practicable, the Chief Information Security Officer will inform Genpact's insurance manager, who will inform Genpact's insurance broker of the incident. The Risk Council will determine whether to inform the provider(s) of Genpact's insurance coverage for cyber extortion demands and will, to the extent possible, adhere to the requirements of any applicable insurance coverage to obtain written approval to engage any necessary security consultants.

The decision whether to pay any ransom demand will be made taking into account all relevant facts, circumstances, and guidance as the case may warrant, subject to the limitation that Genpact will not make or cause to be made any payment that would knowingly violate any applicable law, including economic sanctions laws. Relevant facts and circumstances include, but are not limited to, whether data has been encrypted and/or exfiltrated at the time of the demand, the scope of data involved, the criticality of data involved, the existence of data back-ups, and any information known about the party or parties making the ransom demand.

Genpact's Risk Council will determine whether to engage security consultants and/or brokers specialized in ransomware demands, taking into consideration the requirements of the applicable insurance policy.

Using the risk-based prioritization criteria above, the following approval process will be followed:

- For ransom demands of up to $100,000 and that would have no more than a “medium” risk rating score as defined above, the Chief Financial Officer and Chief Legal Officer may approve the company’s actions.
- For ransom demands that are greater than $100,000 and up to $1,000,000 and that would have no more than a “medium” risk rating score as defined above, the Risk Council may approve the company’s actions in response to the ransom demand.
- For ransom demands that are greater than $1,000,000 and up to $5,000,000, or for demands of any amount up to $5,000,000 that would have a “high” or “critical” risk rating, the Chief Executive Officer may approve the company’s actions in response to the ransom demand.
- For ransom demands that are greater than $5,000,000, the Audit Committee may approve the company’s actions in consultation with the Chief Executive Officer.

The presumption is that for a “low” risk situation, Genpact would not pay ransom.

Governance

Governance for Information Security Plan and overall Information Security at Genpact resides with the **Chief Information Security Officer (CISO)**. **CISO** (SVP Global Information Security and Data Privacy) is responsible to ensure that the overall Cyber Incident Response processes, including this document are operationalized, are reviewed periodically and updated as needed to ensure relevance and continued effectiveness in a very dynamic threat environment.

The results of actual incidents as well as simulations conducted, and lessons learned will be presented to the Information Security Governance Council.

Incident Response Plan Maintenance

The Incident Response plan will be reviewed at minimum annually. All changes to the Genpact Information Security Incident Response Plan will be communicated to all personnel responsible for its implementation and operations. The Communications Contact list will be reviewed quarterly to validate its scope and confirm that accurate personnel contact information is included (e.g., names, department, titles, email addresses, phone numbers).

Incident Response Plan Testing

The Plan shall be exercised annually at a minimum. The exercises are designed to obtain an understanding of how Genpact’s people, processes, and technology withstand the rigors of real-world scenarios. This exercise also serves to fulfil requirements established in Genpact corporate policies, as well as regulatory requirements applicable to Genpact. The response to/learning from an actual incident may serve to fulfil this requirement. The scenarios for the simulation exercises are created based on the real-world security incident situations and preceding incidents.

Incident Metrics

IR Team members are responsible for analysing data related to the Incident Response program to ascertain its performance and enable the program to respond and contain threats faster. The following are key measurements that will be collected by the Incident Management system.

Metric	Formulation
Time to Detect	Detection Time – Actual Occurrence Time
Time to Respond	Investigation Start Time – Detection Time
Time to Contain	Incident Contained Time – Investigation Start Time
Time to Close	Incident Closure Time – Detection Time

Incident Review Process

It is necessary to perform a complete review of the entire incident management life cycle process pertaining to each recorded incident in the incident management tool. The owner of the incident should make sure that each task assigned for the specific incident is completed as per the investigation conducted. Post this, the owner should submit the incident for a review process. The tasks and the recording of artefacts shall be reviewed by supervisor/team member. Once the review process is completed the incident can be marked as closed.

A Dashboard containing the critical security incidents, incident metrics (Technology and Risk wise), Alert and Incident Trends is presented to the InfoSec Leadership on monthly basis.

Escalation Matrix

Escalation matrix is maintained at the below SharePoint location

Escalation Matrix

Communication Matrix

Communication matrix is maintained at the below SharePoint location

Communication Matrix

Appendices

Appendix A: GENPACT Privacy Incident & Breach Response Plan
Appendix B: Chain of Custody

Thank you.