# Planning

- Pandemic Response Planning Policy
- Disaster Recovery Plan Policy
- Security Response Plan Policy

# Pandemic Response Planning Policy

This policy is intended for companies that do not meet the definition of critical infrastructure as defined by the federal government. This type of organization may be requested by public health officials to close their offices to non-essential personnel or completely during a worst-case scenario pandemic to limit the spread of the disease. Many companies would run out of cash and be forced to go out of business after several weeks of everyone not working. Therefore, developing a response plan in advance that addresses who can work remotely, how they will work and identifies what other issues may be faced will help the organization survive at a time when most people will be concerned about themselves and their families.

Disasters typically happen in one geographic area. A hurricane or earthquake can cause massive damage in one area, yet the worst damage is usually contained within a few hundred miles. A global pandemic, such as the 1918 influenza outbreak which infected 1/3 of the world’s population, cannot be dealt with by failing over to a backup data center. Therefore, additional planning steps for IT architecture, situational awareness, employee training and other preparations are required.

This document directs planning, preparation and exercises for pandemic disease outbreak over and above the normal business continuity and disaster recovery planning process. The objective is to address the reality that pandemic events can create personnel and technology issues outside the scope of the traditional DR/BCP planning process as potentially 25% or more of the workforce may be unable to come to work for health or personal reasons.

The planning process will include personnel involved in the business continuity and disaster recovery process, enterprise architects and senior management of <Company Name>. During the implementation of the plan, all employees and contractors will need to undergo training before and during a pandemic disease outbreak.

<Company Name> will authorize, develop and maintain a Pandemic Response Plan addressing the following areas:

The Pandemic Response Plan leadership will be identified as a small team which will oversee the creation and updates of the plan. The leadership will also be responsible for developing internal

expertise on the transmission of diseases and other areas such as second wave phenomenon to guide planning and response efforts. However, as with any other critical position, the leadership must have trained alternates that can execute the plan should the leadership become unavailable due to illness.

The creation of a communications plan before and during an outbreak that accounts for congested telecommunications services.

An alert system based on monitoring of World Health Organization (WHO) and other local sources of information on the risk of a pandemic disease outbreak.

A predefined set of emergency polices that will preempt normal <Company Name> policies for the duration of a declared pandemic. These polices are to be organized into different levels of response that match the level of business disruption expected from a possible pandemic disease outbreak within the community. These policies should address all tasks critical to the continuation of the company including:

How people will be paid

Where they will work – including staying home with or bringing kids to work.

How they will accomplish their tasks if they cannot get to the office

A set of indicators to management that will aid them in selecting an appropriate level of response bringing into effect the related policies discussed in section 4.4—for the organization. There should be a graduated level of response related to the WHO pandemic alert level or other local indicators of a disease outbreak.

An employee training process covering personal protection including:

Identifying symptoms of exposure

The concept of disease clusters in day cares, schools or other gathering places

Basic prevention - limiting contact closer than 6 feet, cover your cough, hand washing

When to stay home

Avoiding travel to areas with high infection rates

A process for the identification of employees with first responders or medical personnel in their household. These people, along with single parents, have a higher likelihood of unavailability due to illness or child care issues.

A process to identify key personnel for each critical business function and transition their duties to others in the event they become ill.

A list of supplies to be kept on hand or pre-contracted for supply, such as face masks, hand sanitizer, fuel, food and water.

IT related issues:

Ensure enterprise architects are including pandemic contingency in planning

Verification of the ability for significantly increased telecommuting including bandwidth, VPN concentrator capacity/licensing, ability to offer voice over IP and laptop/remote desktop availability

Increased use of virtual meeting tools – video conference and desktop sharing

Identify what tasks cannot be done remotely

Plan for how customers will interact with the organization in different ways

The creation of exercises to test the plan.

The process and frequency of plan updates at least annually.

Guidance for auditors indicating that any review of the business continuity plan or enterprise architecture should assess whether they appropriately address the <Company Name> Pandemic Response Plan.

Compliance Measurement

The Precision Computer team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Any exception to the policy must be approved by the Precision Computer team in advance.

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

World Health Organization

The following definition and terms can be found in the SANS Glossary located at:

https://www.sans.org/security-resources/glossary-of-terms/

Pandemic

# Disaster Recovery Plan Policy

Since disasters happen so rarely, management often ignores the disaster recovery planning process.  It is important to realize that having a contingency plan in the event of a disaster gives <Company Name> a competitive advantage.  This policy requires management to financially support and diligently attend to disaster contingency planning efforts.  Disasters are not limited to adverse weather conditions.  Any event that could likely cause an extended delay of service should be considered.  The Disaster Recovery Plan is often part of the Business Continuity Plan.

This policy defines the requirement for a baseline disaster recovery plan to be developed and implemented by <Company Name> that will describe the process to recover IT Systems, Applications and Data from any type of disaster that causes a major outage.

This policy is directed to the IT Management Staff who is accountable to ensure the plan is developed, tested and kept up-to-date.  This policy is solely to state the requirement to have a disaster recovery plan, it does not provide requirement around what goes into the plan or sub-plans.

4.1 Contingency Plans

The following contingency plans must be created:

Computer Emergency Response Plan: Who is to be contacted, when, and how? What immediate actions must be taken in the event of certain occurrences?

Succession Plan: Describe the flow of responsibility when normal staff is unavailable to perform their duties.

Data Study: Detail the data stored on the systems, its criticality, and its confidentiality.

Criticality of Service List: List all the services provided and their order of importance.

It also explains the order of recovery in both short-term and long-term timeframes.

Data Backup and Restoration Plan: Detail which data is backed up, the media to which it is saved, where that media is stored, and how often the backup is done.  It should also describe how that data could be recovered.

Equipment Replacement Plan: Describe what equipment is required to begin to provide services, list the order in which it is necessary, and note where to purchase the equipment.

Mass Media Management: Who is in charge of giving information to the mass media?

Also provide some guidelines on what data is appropriate to be provided.

After creating the plans, it is important to practice them to the extent possible. Management should set aside time to test implementation of the disaster recovery plan. Table top exercises should be conducted annually. During these tests, issues that may cause the plan to fail can be discovered and corrected in an environment that has few consequences.

The plan, at a minimum, should be reviewed an updated on an annual basis.

Compliance Measurement

The Precision Computer team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Any exception to the policy must be approved by the Precision Computer Team in advance.

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

The following definition and terms can be found in the SANS Glossary located at:

https://www.sans.org/security-resources/glossary-of-terms/

Disaster

# Security Response Plan Policy

A Security Response Plan (SRP) provides the impetus for security and business teams to integrate their efforts from the perspective of awareness and communication, as well as coordinated response in times of crisis (security vulnerability identified or exploited). Specifically, an SRP defines a product description, contact information, escalation paths, expected service level agreements (SLA), severity and impact classification, and mitigation/remediation timelines. By requiring business units to incorporate an SRP as part of their business continuity operations and as new products or services are developed and prepared for release to consumers, ensures that when an incident occurs, swift mitigation and remediation ensues.

The purpose of this policy is to establish the requirement that all business units supported by the Precision Computer team develop and maintain a security response plan. This ensures that security incident management team has all the necessary information to formulate a successful response should a specific security incident occur.

This policy applies any established and defined business unity or entity within the <Company Name>.

The development, implementation, and execution of a Security Response Plan (SRP) are the primary responsibility of the specific business unit for whom the SRP is being developed in cooperation with the Precision Computer Team. Business units are expected to properly facilitate the SRP for applicable to the service or products they are held accountable. The business unit security coordinator or champion is further expected to work with the <organizational information security unit> in the development and maintenance of a Security Response Plan.

Service or Product Description

The product description in an SRP must clearly define the service or application to be deployed with additional attention to data flows, logical diagrams, architecture considered highly useful.

4.2 Contact Information

The SRP must include contact information for dedicated team members to be available during non-business hours should an incident occur and escalation be required. This may be a 24/7 requirement depending on the defined business value of the service or product, coupled with the impact to customer. The SRP document must include all phone numbers and email addresses for the dedicated team member(s).

4.3 Triage

The SRP must define triage steps to be coordinated with the security incident management team in a cooperative manner with the intended goal of swift security vulnerability mitigation. This step typically includes validating the reported vulnerability or compromise.

4.4 Identified Mitigations and Testing

The SRP must include a defined process for identifying and testing mitigations prior to deployment. These details should include both short-term mitigations as well as the remediation process.

4.5 Mitigation and Remediation Timelines

The SRP must include levels of response to identified vulnerabilities that define the expected timelines for repair based on severity and impact to consumer, brand, and company. These response guidelines should be carefully mapped to level of severity determined for the reported vulnerability.

Compliance Measurement

Each business unit must be able to demonstrate they have a written SRP in place, and that it is under version control and is available via the web.  The policy should be reviewed annually.

Exceptions

Any exception to this policy must be approved by the Precision Computer Team in advance and have a written record.

Non-Compliance

Any business unit found to have violated (no SRP developed prior to service or product deployment) this policy may be subject to delays in service or product release until such a time as the SRP is developed and approved. Responsible parties may be subject to disciplinary action, up to and including termination of employment, should a security incident occur in the absence of an SRP