Consensus Policy Resource Community

Pandemic Response Planning
Policy

Free Use Disclaimer: *This policy was created by or for the SANS Institute for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to* [*policy-resources@sans.org*](mailto:policy-resources@sans.org)*.*

Last Update Status: *Updated Mar 2020*

1. Overview

This policy is intended for companies that do not meet the definition of critical infrastructure as defined by the US 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 pandemic to lower the immediate risk and 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.

2. Purpose

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 Disaster Recovery/Business Continuity Planning process as potentially some if not the entire workforce may be unable to come to work for health or personal reasons.

3. Scope

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.

4. Policy

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

4.1 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.

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

4.3 An alert system based on monitoring of World Health Organization (WHO), the Centers for Disease Control (CDC) and other Federal, State and Local sources of information on the risk of a pandemic disease outbreak.

4.4 A predefined set of emergency policies that will preempt normal <Company Name> policies for the duration of a declared pandemic. These emergency policies 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:

a) How people will be paid

b) Where people will work – including staying home with or bringing kids to work

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

d) What work will be suspended during the pandemic

e) Communication plan and cadence throughout the pandemic

f) Alternate means to communicate during the pandemic

g) What operational procedures may need to be altered, amended, or suspended, such as those over facilities, visitors, and non-essential activities and events

4.5 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 authoritative indicators of a disease outbreak.

4.6 An employee training process covering personal protection including:

a) Identifying and broadly communicating the symptoms of exposure

b) The concept of disease clusters in daycares, schools or other large gatherings

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

d) When to stay home along with encouragement to do so

e) Avoiding travel to all areas with high infection rates

4.7 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.

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

4.9 A list of supplies to be kept on hand or pre-contracted for supply, such as face

masks, hand sanitizer, fuel, food and water.

4.10   IT related issues:

    a) Ensure enterprise architects are including pandemic contingency in planning

    b) 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

    c) Increased use of virtual meeting tools that facilitate video conference and desktop sharing capabilities

    d) Identify what tasks cannot be done remotely

    e) Pre-negotiated arrangements with key vendors in the event current licensing will not meet this change in work force habits

    f) Determine if any IT colleagues need to remain onsite to support critical operations

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

    h) Expectations concerning printing work documents on personal printers

    i) Expectations about sending work emails and documents to personal email accounts

4.11   The creation of exercises to test the plan in advance.

4.12   Performing a retrospective review to identify and solve for issues encountered in the test

4.13   The process and frequency of plan updates and review at least annually with appropriate approvals or sign-off from organizational leadership or oversight.

4.14   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.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec 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.

5.2 Exceptions

Any exception to this policy must be approved by the <company leadership> team in advance and revalidated annually.

5.3 Non-Compliance

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

6 Related Standards, Policies and Processes

World Health Organization

Centers for Disease Control and Prevention

7 Definitions and Terms

The following definition and terms can be found in the SANS Glossary
located at: https://www.sans.org/security-resources/glossary-of-terms/

- Pandemic

8 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to a new format.
Mar 2020	Russell Eubanks and Trip Hillman	Updated to reflect current learnings from COVID-19.