

INCIDENT-SPECIFIC ANNEX 3—CYBER INCIDENT

LEAD AGENCY

Pierce County Finance Department-Information Technology

SUPPORT AGENCIES

Pierce County Department of Emergency Management
South Sound 9-1-1
Pierce County Departments and Agencies

I. INTRODUCTION

A. Background

Cyber or cyberspace can be compared to the nervous system – the control system – of the nation’s critical infrastructure. Cyberspace is comprised of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructure to work. The nation’s economy and national security are fully dependent upon information technology and the information infrastructure. At the core of the information infrastructure is the internet.

B. Purpose

This incident annex will briefly outline the fundamental steps the Pierce County Information Technology Department (IT) and other supporting agencies will take in preparation for and responding to a cyber incident.

II. POLICIES

A. Pierce County IT will take actions to prepare, within staffing and fiscal constraints, to respond to and recover from all emergencies and disasters impacting the Information Technology (IT) systems and services within Pierce County government.

B. All Pierce County government end-users are responsible for familiarizing themselves with, and complying with, all Pierce County policies, procedures, and standards, dealing with information security.

III. SITUATION

A. Emergency/Disaster Hazards and Conditions

1. The vulnerability of Pierce County IT to an emergency, hazard, or threat, is based on the combination of the probability of an incident occurring and the impact the incident would have on operations.
2. Refer to the Pierce County Hazard Identification and Risk Assessment (published separately).

- B. Planning Assumptions
 - 1. Cyber attacks occur with or without warning.
 - 2. In spite of sophisticated technologies that block many cyber attacks, vulnerabilities exist.
 - 3. An organized cyber attack has the potential to debilitate critical infrastructure, the economy, or national security.

IV. CONCEPT OF OPERATIONS

- A. Pierce County IT provides four main functions:
 - 1. Software development
 - 2. Administration and strategic planning
 - 3. Information technology operations
 - 4. Geographic Information Services
- B. Pierce County IT works with all thirty county departments and over 160 other government jurisdictions and agencies.
- C. Pierce County IT has implemented county-wide policies that address internet access, security, and multiple other related policies.
- D. Pierce County IT has internal continuity of operations and emergency response plans. These documents address specific essential functions, personnel, and emergency actions required to maintain the essential functions required to keep Pierce County government operational.
- E. Pierce County IT maintains vigilant monitoring to detect malicious codes and bots that can negatively impact the county's IT capabilities.

V. RESPONSIBILITIES

- A. Primary Agency
 - Pierce County Information Technology
 - 1. Provide staffing for the EOC that are a part of all EOC activations.
 - 1. Maintain a method of information technology oversight in the form of an Information Technology Committee. This committee is intended to be a forum for county departments to give direction and provide oversight by making resource and priority decisions for the work done by Finance-IT and to provide discussion on products and services provided by the department.

2. Work with appropriate law and legal authorities in the investigation phase of the cyber incident.
- B. Support Agencies
1. Pierce County Department of Emergency Management
 - a. Maintain a functioning IT workstation in the EOC.
 - b. Open the EOC in support of a cyber incident response when warranted. Be prepared to conduct EOC operations without the current computer systems, as they may be compromised in the cyber incident.
 2. South Sound 9-1-1
 - a. Comply with all applicable information technology policies and procedures intended to protect critical emergency communication resources.
 3. Pierce County Departments and Agencies
 - a. Comply with all applicable information technology policies intended to protect critical county IT and communication systems.

VI. AUTHORITIES AND REFERENCES

- Pierce County Charter, Article 9, Section 9.60 – Information Management
- Pierce County Information Technology Continuity of Operations Plan
- Pierce County Information Technology Emergency Response Plan

VII. TERMS AND DEFINITIONS

- (See Appendices I and II)

VIII. ATTACHMENTS

- (None)