ANNEX: MAJOR CYBER INCIDENT

Primary Agency:	Information Services Department
Support Agencies:	Executive Department Police Department All other City Departments

Introduction

Background

The City uses a variety of systems, services, and devices that reply upon both internal and external computer networks in order to function properly. These networks as a whole are commonly referred to "cyberspace" and failures in them, regardless of cause, are commonly referred to as "cyber incidents". Cyber incidents have the potential to disable city services, release non-disclosable information to unknown parties, and create public safety issues, among other things.

Purpose

This incident annex outlines fundamental steps in the City's response to a major cyber incident, including assignment of responsibility and critical actions that must be taken to prepare for, respond to, and recover from a cyber incident.

Policies

- The Information Services Department is responsible for securing and maintaining City information technology assets in accordance with legal requirements and industry standard best practices. They are further responsible for developing and implementing policies and procedures that ensure the City's ability to prevent, detect, and respond to cyber incidents.
- All employees, volunteers, and others with access to City computer systems are required to be familiar with and comply with all policies and procedures related to information technology use and security.
- All City departments are expected to actively participate in continuity of operations planning that accounts for loss of or temporarily unavailable technology services. Continuity of operations planning must include identification of critical services and procedures for continuing those services during the loss of some or all of the City's cyber infrastructure.

Situation and Assumptions

Emergency Conditions

The City's vulnerability to a major cyber incident is directly related to the amount of planning and prevention activities that have been undertaken and the degree to which system users are able to rapidly detect, isolate, and report potential incidents. Emergency conditions related to a major cyber incident may be created from both internal and external sources and which have the potential to cause critical life safety and other essential services to fail.

Planning Assumptions

- The City has a robust cyber security and computer/internet use policy that is regularly updated to reflect best practices.
- The City provides training to all system users on information security, acceptable use policies, social engineering awareness, and incident identification/notification procedures.
- Major cyber incidents can occur with or without warning.
- Major cyber incidents may be malicious or accidental/inadvertent, but initial response must not be dependent on determining which.
- Cyber vulnerabilities are both technological and human caused and will continue to exist regardless of the number of safeguards put in place and the amount of training conducted.
- Regardless of cause, major cyber incidents have the potential to shutdown critical infrastructure, negatively affect life safety, reveal protected information, and to cause harm to people, data, and physical assets.
- Incidents may start and end on systems that are outside of the City's direct control.
- Close coordination with county, state, federal government partners, as well as private sector entities and NGOs will likely be required in a major cyber incident.

Concept of Operations

- The City's Information Services Department provides the following services to support all City departments:
  - Voice and data communication systems
  - File and print systems
  - Wired and wireless networks
  - Servers and file storage
  - Routers, switches, gateways, and firewalls
  - Business systems support, application software development, databases
  - GIS systems and services
  - Access to the internet and inter-governmental networks
- Information Services Department issues contracts for certain types of work and services, including:
  - Software/hardware maintenance
  - Print/copier maintenance
  - Software/database hosting
  - Network security
  - Internet services
  - Phone services
- Information Services routinely works with other government organizations to exchange information best practices.
- Information Services works in conjunction with Emergency Management to assist departments in developing appropriate expectations and continuity of operations plans.

- Information Services bases its own continuity of operations plan upon the needs of other City departments.
- Information Services maintains detailed, confidential procedures for cyber incident response that are based on current best practices.
- Information Services maintains non-disclosable lists of available cyber incident detection and response resources, including tools and outside vendors.
- Information Services utilizes up-to-date services, tools and techniques to detect adverse events on their networks and other systems.
- All system users are trained and know when and how to report possible cyber incidents and how to avoid common network intrusion and social engineering techniques.

Responsibilities

Information Services Department

- Serve as the lead department for major cyber incident response and provide:
  - Subject matter expertise to the ECC and key decision-makers.
  - Personnel and technology to detect, isolate, and eliminate threats and to restore systems after the threat has been dealt with.
- Serve as liaison to other cyber response organizations, which may include but is not limited to:
  - Washington State Fusion Center
  - Multi-State Information Sharing and Analysis Center (MS-IASAC)
  - Washington State Cyber Unified Coordination Group (UCG)
  - Hardware and software vendors
  - Cybersecurity vendors
  - Cybersecurity response teams (government, private, or combined)
  - Governing agencies to which the city is required to report a breech

City of Bothell Executive Department

- Serve as lead for managing consequences that extend beyond the direct effects on computers and servers.
  - Manage the ECC.
  - Coordinate briefings for key decision-makers, in coordination with Information Services.
  - Ensure that life safety needs internally and externally are being addressed by appropriate departments or agencies.
- Serve as liaison to other emergency management organizations, which may include but is not limited to:
  - Other City ECCs/EOCs
  - King County Emergency Coordination Center
  - Snohomish County Emergency Operations Center
  - Washing State Emergency Operations Center
  - Private sector ECCs/EOCs
- Coordinate with Public Information Officer, for release to public, appropriate information and/or notification to individuals of protected information release.

City of Bothell Police Department

- Serve as lead for any criminal investigation that results from the incident and is within the City’s jurisdiction.
    - Provide law enforcement subject matter expertise to the ECC.
    - Conduct criminal investigations pursuant to established policies and procedures.
    - Serve as a liaison to other law enforcement entities with a role in cyber incident response, which may include but is not limited to:
        - Washington State Fusion Center
        - FBI Joint Cyber Task Force (CTF)
        - Washington State Patrol High Tech Crimes United (WSP HTCU)
        - Other local or county law enforcement agencies

All City Departments

- Provide representation to the ECC, as needed.
- Implement Continuity of Operations plans, as required.