WEST COAST DISTRICT MUNICIPALITY

ICT CHANGE CONTROL POLICY

Contents

1. DEFINITIONS. 2
2. INTRODUCTION AND PURPOSE. 2
3. SCOPE AND APPLICABILITY. 2
4. POLICY STATEMENTS. 2
5. PROCEDURES. 3
6. POINTS OF CONTACT. 4
7. REFERENCES AND RELATED POLICIES. 4

Council Resolution: **ITEM 22/08/24/9.1.6**

1. DEFINITIONS

Change Control Process is a procedure that governs the implementation of modifications to any Information Technology system. The procedure will emphasize appropriate documentation and authorization of the change.

Emergency Change is any change that cannot go through the full change control process.

2. INTRODUCTION AND PURPOSE.

It is the policy of West Coast District Municipality (WCDM) to protect the confidentiality, integrity, and availability of information stored, transmitted, or processed by the municipality. The Information Technology (IT) section is responsible for maintaining the security and stability of WCDM computer systems and networks.

This policy covers the requirements needed to document, communicate, and control changes to all network-based Municipality applications, systems, and devices. This policy will help ensure changes occur securely, reliably, and with proper authorization and notification.

3. SCOPE AND APPLICABILITY.

This policy applies to all users of WCDM networks and computing equipment. This policy applies to all computing devices that are owned by WCDM or attached to municipality networks. It applies to all applications in a production state, as well as all devices including, but limited to, servers, workstations that may provide server functionality to clients on the WCDM network, and all network devices. This policy also includes operating system changes and upgrades.

This policy does not apply to computers that are personally owned by officials and are only attached to wireless networks that the municipality provides for public or official use.

4. POLICY STATEMENTS.

a) Changes to information technology systems, which include servers, applications, and/or network environments, that can affect normal operations must go through a change control process prior to deployment.

b) A change control process must be documented for each WCDM device or system.

c) Separation of duties are recognized so that the persons making the hardware, software, or network changes are not approvers of the same change.

d) Software, hardware, or network changes must be tested and approved by the requestor whenever possible before the final changes are applied.

5. PROCEDURES.

1. The Information Technology Change Control Process may be unique to each device or system, but at a minimum it will include the following:
    a) A request for upgrade or modification is made in writing for any information system;
    b) Firewall updates or changes will be documented. An IT Services Request form will be completed for any changes;
    c) Approval for the upgrade or modification is needed from the Director of the affected Department;
    d) Approval and denial of upgrades and/or changes are documented;
    e) Change Control Documentation is created. This documentation will include date, time, server, application, user group, upgrade/change process, and approvals;
    f) An email is sent to all affected users which notifies them of the downtime associated with implementing the change. This email will state the reason for downtime, the affected systems, and the expected outage dates and times;
    g) If additional outages occur due to an unforeseen problem during a change, an email will be sent to the affected users, the Director Financial Services, and the Manager Information Technology. This email will explain the reasoning for the extended outage;
    h) When the system change is complete, the Change Control Documentation will be signed and dated by the employee performing and/or supervising the modification;
    i) Change Control documentation will be stored in a centralized location for future reference;
    j) A final email is communicated to all affected users, the CFO (Chief Financial Officer), and the Manager Information Technology when all modifications have been completed.
    k) Change control documentation will be Archived for future reference.

2. The Information Technology Emergency Change Control Process will include the following:
    a. Emergency changes must have approval from the CFO or Manager Information Technology or the Head of Department which is being affected and must be documented in an IT Request Form describing the problem, the date and time, and the affected system.
    b. Emergency changes must be communicated to the affected users, the Manager Information Technology and the HOD, even after the emergency repair has taken place.

6. POINTS OF CONTACT

Network Administrator
Manager Information Technology
CFO/Director Finance

7. REFERENCES AND RELATED POLICIES

Information Technology Services Change Control Form