BERGRIVIER MUNICIPALITY

PATCH MANAGEMENT POLICY

APRIL 2012

CONTENTS

Revision History

Revision date	Author	Summary of Changes	Changes marked

Approvals This document requires the following approvals.

Name	Signature	Title	Date of Issue	Version

Purpose

This document aims to set out a policy to mitigate the phenomena of vulnerabilities within the Microsoft operating system code within computer and servers on the Bergrivier Municipal (BM) network.

Scope

The scope of this policy is to ensure all computer devices (including servers, desktops, printers, etc.) connected to the BM network have proper virus protection software, current virus definition libraries, and the most recent operating system and security patches installed.

e-Innovation Responsibility

The IT Department is responsible for the overall patch management implementation, operations, and procedures. While safeguarding the network is every network user's responsibility, IT Department ensures all known and reasonable defenses are in place to reduce network vulnerabilities while keeping the network operating. This responsibility includes the tasks detailed below.

Monitoring

The IT Department will monitor security mailing lists, review vendor notifications and Web sites, and research specific public Web sites for the release of new patches. Monitoring will include, but not be limited to, the following:

- Scanning BM network to identify known vulnerabilities.
- Identifying and communicating identified vulnerabilities and/or security breaches to the Head of Department.

Review and Evaluation

Once alerted to a new patch, IT Department will download and review the new patch. The IT Department will categorize the criticality of the patch according to the following:

- **Emergency**—an imminent threat to BM network
- **Critical**—targets a security vulnerability
- **Not Critical**—a standard patch release update
- **Not applicable** to BM environment

Regardless of platform or criticality, all patch releases will follow a defined process for patch deployment that includes assessing the risk, scheduling, installing, and verifying.

Risk Assessment and Testing

The IT Department will assess the effect of a patch to the corporate infrastructure prior to its deployment. The department will also assess the affected patch for criticality relevant to each platform (e.g., servers, desktops, printers, etc.).

If the IT Department categorizes a patch as an Emergency, the directorate considers it an imminent threat to the BM network. Therefore, BM assumes a greater risk by not implementing the patch than waiting to assess it before implementing.

Patches deemed Critical or Not Critical will undergo assessment for each affected platform before release for implementation. The directorate must complete validation against all images (e.g., Windows, etc.) prior to implementation.

Notification and Scheduling

The IT Department must approve the schedule prior to implementation. Regardless of criticality, each patch release requires the creation and approval of a request for technical change (RTC) prior to releasing the patch.

Implementation

As Emergency patches pose an imminent threat to the network, the release must be assessed before installation. In all instances, the directorate will perform assessment (either pre- or post-implementation) and document it for auditing and tracking purposes.

The IT Department will obtain authorization for implementing Critical patches via an emergency RTC and IT Department's approval. The department will implement Not Critical patches during regularly scheduled preventive maintenance. Each patch will have an approved RTC.

For new network devices, each platform will follow established procedures to ensure the installation of the most recent patches.

Auditing, Assessment and Verification

Following the release of all patches, the IT Department staff will verify the successful installation of the patch and that there have been no adverse effects.

User Responsibility and Practices

It is the responsibility of each user—both individually and within the organization—to ensure prudent and responsible use of computing and network resources.