# BERGRIVIER MUNICIPALITY

# OPERATING SYSTEM BASELINE POLICY

## APRIL 2012

# OPERATING SYSTEM BASELINE POLICY

| REVISION NUMBER | DATE | AUTHORISED FOR DISTRIBUTION |
|---|---|---|
| | | |

## 1. PURPOSE

This policy establishes standards for the creation, maintenance and use of secure server OS and network device baselines.

## 2. DEFINITIONS

- Server Operating System Baseline Configuration (Server OS Baseline)
  The minimum configuration of an operating system that meets security and operational requirements. This baseline serves as the starting point for the configuration of different types of servers used to process Bergrivier Municipality information across the network.

- Network device
  Something which mediates data in a computer network and which is configurable beyond simple firmware.

- Certification
  A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

## 3. SCOPE

The provisions of this policy will apply to all server and applicable network device operating systems at Bergrivier Municipality include:

- Those approved and documented.

- Those utilized in development, testing or production environments.

- Those used for Infrastructure support.

## 4. POLICY

### 4.1 GENERAL POLICY

A secure configuration baseline will be defined and documented for each server operating system. The development and documentation of a secure baseline configuration for other network devices such as switches is highly recommended. The secure baseline configuration may be customized to fit technical, architectural, and operational constraints. The secure baseline will address all aspects of the OS and device configuration including but not limited to:

- Configuration of security controls.

- Elimination of unnecessary services and utilities.
- Configuration requirements for allowed services and utilities.
- Standardization of audit logging configurations.
- Application of current vendor recommended patch sets and/or service packs.

A secure baseline will be defined for new operating systems.

The secure baseline will be the minimum configuration for all servers and deployed within Bergrivier Municipality.

All servers and network devices, where practicable, will be updated regularly in accordance with the ***Patch Management Policy.*** Servers and network devices that do not comply with the current secure baseline configuration will be modified to reflect the baseline configuration at the next scheduled security configuration upgrade cycle.

New application development and major changes to existing applications will be required to adopt the current baseline for their selected operating system.

Any hardware systems that cannot operate with the Security OS Baseline will be considered non-compliant and will not be deployed into production.

## 4.2 DOCUMENTATION

Implementation details of the secure baseline for a specific operating system or a specific network device will be documented.

## 4.3 MAINTENANCE OF THE BASELINE

The secure baseline documents will be periodically updated to reflect new security patches installed in accordance with the ***Patch Management Policy.***

## 4.4 EXCEPTIONS

All deviations from the secure baseline required by a new application must be identified and approved by the IT Committee and shall be documented.

If a server or network device requires deviations from the secure baseline due to the incompatibility of an existing application, the deviations will be documented and reported to the IT Committee.

## 5. COMPLIANCE

The Systems Administrator responsible for the installation of an Operating System on a server will certify that the installation is in compliance with this policy.

The Systems Administrator responsible for maintaining a server will certify that the server is maintained in compliance with this policy.

The Network Administrator responsible for maintaining the network will certify that it is maintained in compliance with this policy.

If a network device is opted to employ a secure baseline, the Network Administrator responsible for maintaining that device shall certify the device is maintained in compliance with this policy.

## 6. ROLES AND RESPONSIBILITIES

All employees or contractor employees responsible for the management, testing, evaluation, implementation, installation, configuration, operation, and maintenance or security of IT resources will implement the mandatory practices of this policy and will identify any proposed deviations from the mandatory practices of this policy.

The appropriate system administrators will update the secure baseline, if applicable, to document the patches and service packs deployed in accordance with the ***Patch Management Policy***.

The system administrator installing a new server or network device will certify the secure baseline installation on servers or network device.

The System Administrator maintaining a system is responsible for deploying regular updates in accordance with the ***Patch Management Policy***.