POLICY 021/2015 RAADSBELEID

ONDERWERP: IT-PATCH MANAGEMENT POLICY

VERWYSING: 6.1.B

BESLUIT NR: 27/05.1/2015 (SRV) DATUM: 13 Mei 2015

PURPOSE: This policy defines procedures to be performed allowing for good practice of patch management.

POLICY PHILOSOPHY AND PRINCIPLE

Patch management allows for the updating of information technology components of both hardware and software. Patches are developed for IT components due to the following reasons:

- Rectification of software errors causing malfunctioning
- Curbing the vulnerabilities caused by viruses, malware, and spyware.

Patches can also if not implemented correctly cause functioning software to malfunction. Therefore proper processes must be followed to ensure optimal usage.

GUIDELINES

1. This policy applies to IT hardware and software

2. To ensure optimal output on systems all patches need to be tested before implementing. Tested patches will be approved for implementation.

3. Only authorized persons may update any IT components with any patch.

4. The users of IT components must allow authorized personnel to install patches that have been approved.

PROCEDURE

1. Patch updates are included in the following components and associated patch types:

Component	Patch type
Severs, Computers, printers, faxes, scanners	Drivers, Firmware
Routers, switches, radio equipment	Firmware
Operating Systems	Service packs
Application Software	Feature updates, Service packs

2. The IT Manager ensures that all patches are tested.

3. After testing the IT Manager approves or rejects patch for implementation.

4. IT personnel or contractors are appointed to install the approved patches.

ROLES

IT Manager

IT Personnel
End users

RELATED POLICIES
Besigheidskontinuiteit Beleid
IT Backup Policy

RECALL / CHANGE
This policy replaces any previous policy in this regard.