Server Policy

Introduction

Gemporia recognises that payment card information is a valuable asset. Managing security systems and the information they contain is vital to maintain Gemporia's reputation and the ability to continue trading successfully.

Gemporia considers the security of its cardholder data environment (CDE) and cardholder data to be a crucial element of its business and, to this end, has created a well-defined set of policies, standards and procedures to support secure operations

The aim of this policy document is to lay out how Gemporia will operate its servers in order to uphold security standards required and desired for this role.

Scope

This policy applies to the people, processes and technology that interact directly or indirectly with servers within the CDE, in particular those who configure and install such servers.

This policy document is designed to be used in conjunction with the appropriate implementation standards as defined by Gemporia in accordance with best practices.

Policy Statement

1. New Servers
    1. All new servers must be established in accordance with the "New CDE Component" policy
    2. Servers must be configured in line with The Server Standard document and inline with best practices
2. Physical access
    1. Physical access to servers in the CDE shall be restricted and monitored at all times
3. AntiVirus
    1. All CDE computers/servers shall run and maintain anti-virus software if they can be affected by viruses
    2. Antivirus shall be capable of identifying and removing other malicious software including malware and adware
    3. Antivirus software will automatically update to the latest security definitions on a regular basis as recommended by the vendor, these actions shall be logged
    4. Automated, periodic, scans must be scheduled to run and scan all locally attached storage and memory
    5. Log generation must be stored centrally to for 1 year minimum
4. Patching
    1. Within 30 days of release all Vendor approved patches must be installed unless sound business justification can be provided and a mitigation strategy devised to protect from the identified defect

    2. Appropriate sources will be monitored for high security alerts and appropriate updates installed to mediate them where possible
5. Decommissioning
    1. When decommissioning hardware / software from the CDE environment it must be guaranteed to contain no cardholder data
    2. All passwords and credentials must be removed
    3. All machine based authentication / accounts must be revoked from the network before removal

Revision History

Date	Description	Who
12/08/2015	Original Document	Andrew Smith
13/10/2015	Added 3.2.9	Andrew Smith
02/12/2015	Added 3.3.5	Andrew Smith
08/08/2016	Changed TGGC to Gemporia	Andrew Smith

From:
https://techdocs.amber.cx/ - **Gemporia Wiki**

Permanent link:
https://techdocs.amber.cx/policies/servers

Last update: **2016/11/03 14:42**