Firewall Policy

Responsible Parties

<table>
<thead>
<tr>
<th>Prepared By</th>
<th>Document Version</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kevin Kuhn</td>
<td>Version 1.0</td>
<td>314/977-1786</td>
</tr>
</tbody>
</table>

| Effective Date:   | November 20, 2009 | Last Updated: | November 20, 2009 |
| Divisions or Departments Affected: | Saint Louis University ITS |

| Approved By:      | Tim Brooks, CIO   | Approval Date: | 11-24-09 (Signature On File) |

Audience
This document applies to all Saint Louis University (SLU) ITS network firewalls, systems and applications.

Responsibilities

Executive Sponsor  Saint Louis University

Key Stakeholders  SLU, SLU ITS, Database Administrators, IT Functional Managers and Data Process Owners

Document Owner  SLU ITS Quality Assurance Office

Document Management  SLU ITS is responsible for the publication, notification and maintenance of this document.

Implementers  SLU ITS is responsible for ensuring that the requirements in this document are implemented.

Document Change Record

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>November 20, 2009</td>
<td>Firewall Policy</td>
</tr>
</tbody>
</table>
Table of Contents

REVISION CHART ........................................................................................................ 3
INTRODUCTION ............................................................................................................ 4
PURPOSE ...................................................................................................................... 4
DEFINITIONS & ROLES .............................................................................................. 4
APPLICABILITY ............................................................................................................ 4
FIREWALL POLICY ....................................................................................................... 4
Firewall Audit Logging ................................................................................................ 4
Firewall Changes .......................................................................................................... 4
RESPONSIBILITIES ...................................................................................................... 5
APPROVAL AND AMENDMENTS .............................................................................. 5
APPENDIX .................................................................................................................... 5
## REVISION CHART

<table>
<thead>
<tr>
<th>Version</th>
<th>Primary Author(s)</th>
<th>Description of Version</th>
<th>Date Completed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>K. Kuhn</td>
<td>Initial Version</td>
<td>November 24, 2009</td>
</tr>
</tbody>
</table>

## Document Change Record

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>November 24, 2009</td>
<td>Firewall Policy</td>
</tr>
</tbody>
</table>
INTRODUCTION
Firewalls are an essential component of SLU’s information systems security infrastructure. They are designed to establish a perimeter where access controls are enforced, thus enhancing security of computer and network resources to ensure a more reliable network and reduce illegal and malicious activities.

PURPOSE
The purpose of this policy is to ensure SLU has the proper network perimeter security in place to prevent malicious intrusion while allowing communications necessary to facilitate daily University needs. Furthermore, this policy is designed to help protect electronic information systems and ensure compliance with regulations such as the Health Insurance Portability and Accountability Act (HIPAA), the Family Educational Rights and Privacy Act (FERPA), and Payment Card Industry (PCI) Security Standards.

DEFINITIONS & ROLES
- **Audit Log** – A system that provides a means for tracing items of data from processing step to step, particularly from a machine-produced report or other machine output back to the original source data.
- **Firewall** – A hardware or software device that is designed to block unauthorized inbound network traffic while permitting authorized outbound communications

APPLICABILITY
This policy applies to all SLU and SLUCare information resources and to all users of those resources, whether on University property or from remote locations. Additional policies may apply to specific computers, computer systems, voicemail systems or networks.

FIREWALL POLICY
Network Connections
All external and wireless connections to University networks must pass through a network firewall. The goal of every SLU network firewall is to allow access from our protected environment to the largely unprotected computing environment known as the Internet. This allows authorized access into the SLU environment by users located outside our firewall for the purpose of conducting University business.

Firewall Audit Logging
When applicable, all SLU network firewalls will employ the audit logging feature to show any configuration changes, who made the changes, and when the changes were made. Any willful attempt to turn off the audit logging feature on University-owned firewalls will result in disciplinary action, up to and including termination of employment.

Firewall Changes
All changes to University network firewalls must follow SLU Firewall Change Control Process Standard Operating Procedures. It is the responsibility of the system owner to identify any firewall changes needed for successful project implementation and to schedule sufficient time for such changes to be properly documented, reviewed, and approved.

Firewall Physical Security
All University network firewalls must be physically located in ITS data centers and accessible only to those whose roles and responsibilities permit them to access network firewalls as defined within the SLU Data Center Security Policy.

Document Change Record

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>November 24, 2009</td>
<td>Firewall Policy</td>
</tr>
</tbody>
</table>
RESPONSIBILITIES
It is the responsibility of any person using SLU resources to read, understand, and follow these guidelines. In addition, users are expected to exercise reasonable judgment in interpreting these guidelines and in making decisions about the appropriate use of SLU resources. Any person with questions regarding the application or meaning of these guidelines should seek clarification from his or her supervisor.

APPROVAL AND AMENDMENTS
Changes to this policy may be necessary from time to time. At a minimum, this policy will be reviewed and approved annually. All changes to this policy will be approved by the Chief Information Officer. Documentation, including a record of all changes to the charter, will be maintained by the QA Office and available for inspection for three years.

APPENDIX
Referenced Documents
SLU Firewall Change Control Process Standard Operating Procedures
SLU Data Center Security Policy