MISSISSIPPI VALLEY STATE
UNIVERSITY

# INFORMATION TECHNOLOGY DEPARTMENT

## Restricted List of Ports and Protocols Policy

### General Information

Mississippi Valley State University has adopted the configuration management principles established in NIST SP 800-171 “Configuration Management” control guidelines as the official policy for this security domain. Each system administrator and system owner must adhere to the guidelines and procedures associated with this policy in order to support and be compliant with the University information security framework.

The principle of least functionality provides that information systems are configured to provide only essential capabilities and to prohibit or restrict the use of non-essential functions, such as ports, protocols, and/or services that are not integral to the operation of that information system.

### Purpose

Configure information systems to provide only essential capabilities and specifically prohibit or restrict the use of functions, ports, protocols, and/or services that are not required for the business function of the information system.

### Scope

Disable any functions, ports, protocols, and services within an information system that are deemed to be unnecessary and/or non-secure.

### Policy

MVSU Information Technology Department shall specifically prohibit or restrict the creation of advertised services that open the following functions, ports, protocols, and/or services on a server:

- Background File Transfer Protocol (BFTP) Port 152 / TCP
- Border Gateway Protocol (BGP) Port 179 / Transmission Control Protocol (TCP)
- Courier Port 530 / TCP, User Datagram Protocol (UDP)
- Domain Name System be (DNS) Port 53 / TCP, UDP
- File Transfer Protocol (FTP) Ports 20, 21 / TCP
- Finger Port 79 / TCP
- Hypertext Transfer Protocol (HTTP) Port 80 / TCP; 443 / TCP
- HTTP-MGMT Port 280 / TCP
- Identification Protocol (IDENT) Port 113 / TCP, UDP
- Internet Control Messaging Protocol (ICMP) – block incoming echo requests (ping and Windows traceroute) block outgoing echo replies, time exceeded, and destination

unreachable messages except “packet too big” messages (type 3, code 4). Note: Blocking ICMP will restrict legitimate use of PING in an effort to restrict malicious activity.

- Internet Message Access Protocol (IMAP) Port 143 / TCP, UDP
- Internet Relay Chat (IRC) Port 194 / UDP
- Lightweight Directory Access Protocol (LDAP) Port 389 / TCP, UDP
- Line Printer Daemon (LPD) Port 515 / TCP
- LOCKD Port 4045 / TCP, UDP
- Network Basic Input Output System (NetBIOS) Ports 135, 445 / TCP, UDP; 137-138 / UDP; 139 / TCP
- Network File System (NFS) Port 2049 / TCP, UDP
- Network News Transfer Protocol (NNTP) Port 119 / TCP
- Network Time Protocol (NTP) Port 123 / TCP
- Oracle Names (ORACLENAMES) Port 1575 / TCP, UDP
- Port Mapper (PORTMAP/RPCBIND) Port 111 / TCP, UDP
- Post Office Protocol 3 (POP3) Ports 109-110 / TCP
- Services Ports 512-514 / TCP
- Secure Shell (SSH) Port 22 / TCP
- Session Initiation Protocol (SIP) Port 5060 / TCP, UDP
- Shell Port 514 / TCP
- Simple File Transfer Protocol (SFTP) Port 115 TCP, UDP

**Enforcement**

MVSU Staff members found in policy violation without consulting the MVSU IT Department may be subject to disciplinary action.

**Review**

**This policy will be reviewed annually unless changes are made that require changes prior to the annual review.**