DMZ Security Policy

1.0 Purpose
This policy establishes information security requirements for all networks and equipment deployed in Fuqua located on the "De-Militarized Zone" (DMZ). Adherence to these requirements will minimize the potential risk to Fuqua from the damage to public image caused by unauthorized use of Fuqua resources, and the loss of sensitive/company confidential data and intellectual property.

2.0 Scope
Fuqua networks and devices (including but not limited to routers, switches, hosts, etc.) that are Internet facing and located outside Fuqua internal firewalls are considered part of the DMZ and are subject to this policy. This includes devices in primary Internet Service Provider (ISP) locations and remote locations. All existing and future equipment, which falls under the scope of this policy, must be configured according to the referenced documents. This policy does not apply to devices with private addresses residing inside Fuqua's internet firewalls. Standards for these devices are defined in the Internal Security Policy.

3.0 Policy

3.1. Ownership and Responsibilities
1. All new DMZ devices require a business justification with sign-off at the Assistant Dean of IT level. The IT Infrastructure Team must keep the business justifications on file.
2. Changes to the connectivity and/or purpose of existing DMZ devices and establishment of new DMZ devices must be requested through, and approved by the Fuqua IT Infrastructure Team.
3. The Fuqua IT Infrastructure Team must maintain a firewall device between the DMZ and the Internet.
4. The Fuqua IT Infrastructure Team reserves the right to interrupt connections if a security concern exists.
5. The Fuqua IT Infrastructure Team will provide and maintain network devices deployed in the DMZ up to the OIT point of demarcation.
6. The Fuqua IT Infrastructure Team must record all DMZ device address spaces and current contact information for host and hosted web sites.
7. The Fuqua IT Infrastructure Team is ultimately responsible for all DMZ devices and web sites complying with this policy.
8. Immediate access to equipment and system logs must be granted to members of the Fuqua IT Infrastructure Team upon request, in accordance with the Audit Policy
9. The Fuqua IT Infrastructure Team will address non-compliance waiver requests on a case-by-case basis.

3.2. General Configuration Requirements
1. DMZ devices must not be connected to Fuqua's corporate internal networks, either directly or via a wireless connection.
2. Firewall devices must be configured in accordance with least-access principles and the DMZ business needs. All firewall filters will be maintained by the Fuqua IT Infrastructure Team.
3. The firewall device must be the only access point between the DMZ and the rest of Fuqua's networks and/or the Internet. Any form of cross-connection which bypasses the firewall device is strictly prohibited.
4. Original firewall configurations and any changes thereto must be reviewed and approved by the Fuqua IT Infrastructure Team (including both general configurations and rule sets). The Fuqua IT Infrastructure Team may require additional security measures as needed.
5. Traffic from DMZ to the Fuqua internal network, including VPN access, falls under the Remote Access Policy.
6. Operating systems of all hosts internal to the DMZ running Internet Services must be configured to the secure host installation and configuration standards.
7. Current applicable security patches/hot-fixes for any applications that are Internet services must be applied. Administrative owner groups must have processes in place too stay current on appropriate patches/hotfixes.

8. All applicable security patches/hot-fixes recommended by the vendor must be installed. Administrative owner groups must have processes in place to stay current on appropriate patches/hotfixes.
9. Services and applications not serving business requirements must be disabled.
10. Remote administration must be performed over secure channels (e.g., encrypted network connections using SSH or IPSEC) or console access independent from the DMZ networks.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action up to and including termination of employment.

5.0 Definitions

Terms	**Definitions**
Access Control List (ACL)	Lists kept by routers to control access to or from the router for a number of services (for example, to prevent packets with a certain IP address from leaving a particular interface on the router).
Device	Any network addressable piece of hardware, including but not limited to servers, switches, storage, hardware appliances, etc.
DMZ (de-militarized zone)	Networking that exists outside of Fuqua primary firewalls, but is still under Fuqua administrative control.
Least Access Principle	Access to services, hosts, and networks is restricted unless otherwise permitted.
Internet Services	Services running on devices that are reachable from other devices across a network. Major Internet services include DNS, FTP, HTTP, etc.
OIT Point of Demarcation	The point at which the networking responsibility transfers from Duke OIT to the DMZ. Usually a router or firewall.
Firewall	A device that controls access between networks, such as a PIX, a router with access control lists, or a similar security device approved by InfoSec.

6.0 Revision History

Date	Who made the revision	Change made
2012-01-25	Fuqua Infrastructure	Initial issue