F5 Configuration Standard

Policy Title:
F5 Configuration Standard

Responsible Executive(s):
Chief Information Security Officer

Responsible Office(s):
University Information Security Officer

Contact(s):
If you have questions about this standard, please contact the University Information Security Office.

I. Policy Statement

These standards cover configuration scenarios for applications running through the F5 LTM/ASM Appliance. To ensure applications are configured to only be accessible by necessary networks and have the correct firewall policies applied.

II. Definitions

Character Classes: There are four, character classes available. The four classes are numbers, lowercase letters, uppercase letters, and special characters. Special characters are those characters that can be typed on a computer that do not fall into one of the other three classes.

Student Worker: A student worker is an individual who is enrolled in at least one class at Loyola, is hired in a position that is not eligible for benefits and works in a temporary capacity. This includes hourly employees and temporary part-time (TPT) workers. This does not include permanent part-time (PPT) workers or full time employees (FTE).

Exception Example: If a system treats uppercase and lowercase characters as the same, and does not accept special characters, it is impossible to create a privileged password using our standards. In this case, the password would have a length of eight characters

(matching the standard) and would contain both characters and numbers (2 classes being as close to the standard of 3 as possible).

III. Policy

Scenario 1: Static Web Content

Considerations:

Non-production application

LUC Lakeshore and Water Tower accessibility

No credential pages OR sensitive data

Configuration:

iRule – X-Forwarded-For

iRule – Source 10.0.0.0/8, 147.126.0.0/18, 147.126.64.0/18

Port 80 or 443 with SSL termination

Development

Classification	Considerations	Configuration	Risk
Static Web Content	• Non-production application • LUC accessibility • No credential pages OR sensitive data	• iRule – X-Forwarded-For • iRule – Source Loyola • Port 80 or 443 with SSL termination	Very Low
Authenticated Web Content	• Non-production application • LUC accessibility • Credential pages AND NO sensitive data	• iRule – X-Forwarded-For • iRule – Source Loyola • Port 443 with SSL termination • Port 80 to 443 redirection	Low
Sensitive Web Content	• Non-production application • LUC accessibility	• iRule – X-Forwarded-For • iRule – Source Loyola • Port 443 with SSL pass-through • Port 80 to 443 redirection	Medium

	• Credential pages AND sensitive data		

Production – Internal

Classification	Considerations	Configuration	Risk
Static Web Content	• LUC accessibility • No credential pages OR sensitive data	• iRule – X-Forwarded-For • iRule – Source Loyola • Port 80 or 443 with SSL termination	Low
Authenticated Web Content	• LUC accessibility	•	

IV. Related Documents and Forms

Not applicable.

V. Roles and Responsibilities

Chief Information Security Officer	Enforcing the Standard at the University by setting the necessary requirements.

VI. Related Policies

Please see below for additional related policies:

- Security Policy

Approval Authority:	ITESC	**Approval Date:**	October 29th, 2014
Review Authority:	Jim Pardonek	**Review Date:**	June 17th, 2024
Responsible Office:	UISO	**Contact:**	datasecurity@luc.edu