**Title: Plan for External Penetration Test and Internal Vulnerability Assessment**

**Version: 1.0**

**Date: ddmmyyyy**

**Classification: Internal**

**Document Coordinator: yyyy**

This will be conducted at least once every year between August and September and if there are significant changes to the IT infrastructure. This will cover the following:

* An understanding of any security vulnerabilities associated with accessing the XXXX web facing applications.
* Vulnerabilities in the internal infrastructure.
* Configuration issues with the firewalls.
* Recommended remediation steps to address any issues identified during the assessment.

**Internal Vulnerability Assessment:**

* 250 IP addresses.
* Includes servers and databases, network devices and user's systems.
* 4 VLANs.
* All located within ----
* Testing will be required from onsite at ----

**Build & Configuration Review:**

* 1 Sonic Wall firewall.
* 82 firewall rules

**External Penetration Testing**

• Full Automated and Manual assessment

• 6 hosts in the DMZ within two subnets (3x Linux servers (xxx.xx.xxx.x xxx) & 3x Windows servers (xxx.xx.xxx.x xxx). Assessment to determine what an Internet based attacker without credentials could determine about the target hosts as a preliminary to a potential attempt to compromise them

• Firewall non-whitelisted

• IPS / IDS whitelisted

**Web Application Testing**

The web application testing will cover the 10 top OWASP vulnerabilities

The web applications to be assessed using Grey Box testing are as follows: