\_Networking Management & Security Policy\_

A Policy for Network Management and Security by Joel Parkinson

The following policy will cover the following things regarding network management and security.

* Periodic Reviews of Groups Access Levels and User Access Rights.
* Periodic Penetration Testing.
* Periodic Security Audits.
* Periodic Reviews of Firewalls and Access Control List Policies.

# Sports4U Network Management & Security Policy 2016

All Networking managers within the Sports4U organisation must comply with the following policy requirements to ensure all networks stay secure at all times.

* (1) All group and individual user access rights must be checked thoroughly upon the Sports4U network system. User access rights must conform to the position of which the individual user currently holds within the company. Group access rights must also be checked to ensure that all groups that individual users are a part of do not have any rights above what they’re required to have and also have a high enough access level to ensure maximum productivity.
  + Section 1 of this policy should be undertaken once per month.
  + On the event of a new employee being employed, this section should also be undertaken again for all groups and users that are effected by the new employee’s employment.
  + On The event of any unforeseen system downtime or system updates/upgrades, this section should also be undertaken again.
* (2) Periodic penetration testing should be undertaken once every month or in the event of any upgrades/updates to the networking system. This testing should cover the following:
  + Firewall Penetration testing.
  + Password Vulnerabilities.
  + Anti-Virus Scans. (Full System)
  + Anti-Malware Scans. (Full System)
* (3) Periodic Security Audits must be undertaken once every 3 months to ensure that the Sports4U companies informational systems conform to the set of established criteria as set in the previously set security audit.
* (4) A review of the Sports4U’s firewall status and access control list policies should be undertaken once per month to ensure that the firewall is blocking all incoming & outgoing data except that which pertains to the Sports4U company. All Incoming and Outgoing data should be blocked, allowing only the following:
  + HTTP web requests for the company website.
  + FTP requests from company personnel (IP range Specific)
  + SQL Requests from the local network only
  + IMAP & SMTP incoming and outgoing data (To be flushed through the Sports4U’s Anti-Virus & Anti-Malware service in a secure zone before allowing access onto the main network.