**15. IDS Policy**

In order to preserve the integrity of data that Familyfirst stores, processes, or transmits for Customers, Familyfirst implements strong intrusion detection tools and policies to proactively track and retroactively investigate unauthorized access. Familyfirst currently utilizes [OSSEC](http://www.ossec.net/) to track file system integrity, monitor log data, and detect rootkit access.

**15.1 Applicable Standards**

**15.1.1 Applicable Standards from the HITRUST Common Security Framework**

• 09.ab - Monitoring System Use

• 06.e - Prevention of Misuse of Information

• 10.h - Control of Operational Software

**15.1.2 Applicable Standards from the HIPAA Security Rule**

• 164.312(b) - Audit Controls

**15.2 Intrusion Detection Policy**

1 OSSEC is used to monitor and correlate log data from different systems on an ongoing basis. Reports generated by OSSEC are reviewed by the Security Officer on a monthly basis.

2 OSSEC generates alerts to analyze and investigate suspicious activity or suspected violations.

3 OSSEC monitors file system integrity and sends real time alerts when suspicious changes are made to the file system.

4 Automatic monitoring is done to identify patterns that might signify the lack of availability of certain services and systems (DoS attacks).

5 Familyfirst firewalls monitor all incoming traffic to detect potential denial of service attacks. Suspected attack sources are blocked automatically. Additionally, our hosting provider actively monitors its network to detect denial of services attacks.

6 All new firewall rules and configuration changes are tested before being pushed into production. All firewall and router rules are reviewed every quarter.

7 Familyfirst utilizes redundant firewall on network perimeters.