Safe•Connect Privacy Statement

Overview

Maintaining the privacy of end users is a primary design consideration and goal of the Impulse Safe•Connect Network Access Control (NAC) System.

The purpose of the Impulse Safe•Connect NAC System is to enable an Institution to take more proactive measures to ensure a secure IT infrastructure. The goal is to provide for an environment free of security threats and vulnerabilities, which promotes the exchange of ideas, information and content to create a positive and productive environment for all parties.

The software installed will not report or log any activity other than what is required to ensure end user compliance with the endpoint security policies set forth by the Institution.

No direct personal information will be collected or stored. In situations where the end user is found to be out of compliance with the institution's stated policy, the Safe•Connect System will warn or quarantine the end user based on the policies configured within the Safe•Connect Policy Management Console.

Real-time policy status metrics of endpoint devices under policy management are kept in a secure database on-premise within the Impulse Safe•Connect Policy Enforcer Appliance. The Safe•Connect system database contains no information that can link it directly back to end user personal content. The data collected is policy status related used for statistical trending only, and designed to enable the enterprise to better support and maintain a secure network environment.

Under certain circumstances end users may be denied network access and quarantined based on the enterprise's acceptable use policy enforcement rules. In such circumstances the system provides remediation guidance to the end user to become compliant with security policy.

Impulse Policy Key

The Impulse Safe•Connect NAC System requires a software component to be installed on the end user's computer system. This Policy Key will establish a connection to the Impulse Safe•Connect Policy Enforcer Appliance to maintain access to the Internet or Intranet resources. The policy key will also monitor certain files, processes or registry settings (as dictated by the enterprise) to assess the endpoint's compliance with acceptable use security policies. If the required existence or configuration of files and records do not meet the institution's policy requirements, the Impulse Safe•Connect Policy Enforcer will be notified and the appropriate actions will be taken in accordance with the rules and regulations set forth by the policy administrator. The policy key will not collect personal information nor does it have the ability to act as spyware. The policy key strictly collects policy status information which is required for the operation of the Impulse Safe•Connect NAC System.

Impulse Safe•Connect Policy Enforcer Appliance

The information stored on the Impulse Safe•Connect Policy Enforcer Appliance (that is resident at the Institution's premise) does not contain any personal end user content information and is used for the sole purpose of monitoring, managing, and maintaining the endpoint IT network access security policies defined by the enterprise.

Third-Party Sites

Please note that other web sites that may be accessed when using our system may collect personally identifiable information about the end user. The information security practices of those third-party web sites accessed in conjunction with the Impulse Safe•Connect NAC System are not covered by this privacy statement.

Cookies

Impulse Point's NAC system or website do not use cookies. Accessing advertising or promotional web sites through the Impulse Point Portal may expose the end user to third-party cookies. If this is objectionable, the end user should set the permission levels at their browser accordingly. Impulse Point has no ability to monitor or control third-party cookie use.