BluTrust Network Security Policy

rev. 08.28.26

This policy supports BluIP's company-wide compliance efforts, including SOC 2, HIPAA, and applicable contractual obligations.

Purpose

This policy establishes BluIP's requirements for deploying, managing, and operating Network Security Controls that protect BluIP systems and data. Inadequate network controls can expose systems to unauthorized access, malicious traffic, service disruptions, and operational risk. The purpose of this policy is to maintain layered, consistent, and secure boundaries across all BluIP networked environments to safeguard system availability, confidentiality, and integrity. [DCF-678]

Scope

Who Needs to Comply

- Technical Personnel responsible for administering and maintaining firewalls, routers, cloud networks, and/or security appliances, including the monitoring, configuration, and review of Network Security Controls.
- Vendors or third parties providing network security tools or managed services

What This Policy Covers

This policy applies to the following systems, technologies, and functional areas:

- Network Security Controls (e.g., firewalls, WAFs, IDS/IPS, cloud network policies)
- network segmentation, boundary protections, and traffic filtering
- network diagrams, data-flow diagrams, and documentation describing trusted/untrusted boundaries
- configuration standards for firewalls, routers, ACLs, cloud VPC/VNet configurations
- logging, monitoring, and management of network perimeter and internal security controls
- network rule review, updates, change control, and administrative access
- protection against malicious, anomalous, or unauthorized network traffic

Where This Policy Applies

- BluIP cloud infrastructure and virtual networks
- On-premises network infrastructure supporting BluIP services
- All internal and external networks
- Any system or environment connected to BluIP's network security enforcement points

Exclusions

- Host-level security not related to network enforcement (see, Endpoint Security Policy)
- Physical security controls (see, Asset Management Policy)
- Vendor network security policies

Policy

BluIP subscribes to a layered defense or defense-in-depth approach to network security; Network Security Controls are an essential layer of BluIP security infrastructure. This policy outlines key requirements for Network Security Controls in scope.

Network Representations

- A representation of the boundaries between the environments, all trusted networks, and all untrusted networks are documented (e.g., network diagram) and kept up to date through periodic reviews and updates upon changes to the environment. [DCF-22]
- A representation of the flow of data between System components and across network segments are documented (e.g., data-flow diagram) and kept up to date through periodic reviews and updates upon changes to the environment. [DCF-204]

Network Security Controls

- Network Security Controls are deployed to protect BluIP systems from intrusion, suspicious anomalies, threats and block harmful traffic.
- Network Security Controls are implemented to limit inbound and outbound traffic to the environment to what appears necessary based on business justification. Other traffic is denied through default deny-all rules.
- BluIP Servers are protected with BluIP network perimeter (e.g., Network Perimeter Firewalls), and host-based security controls (e, g., Host-Based Firewalls).
- Network Security Controls will have been implemented between trusted and untrusted networks to endeavor to prevent unauthorized traffic from traversing network boundaries.
- Network Security Controls have been implemented to restrict inbound traffic from untrusted networks to trusted networks to communications with system components that are authorized to provide services, protocols, and ports, and stateful responses to communications initiated by system components in a trusted network. Other traffic is denied.
- Unauthenticated inbound connections is blocked by default.
- Web Application Firewalls have been deployed to as protection from external attacks.

    Associated control: DCF-748

Configuration Standards

- Configuration standards for Network Security Controls, including configurations for firewalls, routers configured with access control lists, and cloud virtual networks have been documented and implemented.
- All services, protocols, and ports allowed have been identified, documented, approved, and have a defined business need.
    - Inbound Firewall rules have been approved and documented by an authorized person; the business need is included in the documentation. [DCF-85]

- Configuration files for Network Security Controls (including files, automated and System-based controls, scripts, settings, infrastructure as code, or other parameters used to configure and synchronize Network Security Controls) are secured from unauthorized access and kept consistent with active network configurations.

Maintenance of Network Security Controls

- All changes to network connections and to configurations of Network Security Controls are documented, approved, and managed in accordance with the Change Management Policy.
- Network Security Control rulesets are reviewed weekly.
- Unnecessary Firewall rules that are no longer needed are removed or disabled.
- Administrative access to firewalls is be logged and the logs monitored. Access to both firewall and ruleset configurations are reviewed weekly.

Monitoring of Activity

Intrusion-detection and/or intrusion-prevention techniques are configured to keep engines, baselines, and signatures up to date.

Firewall and System Administrators

Personnel that administer Firewalls and Systems are responsible for adherence to this policy.

Information Technology Services (ITS)

Anyone who has reason to suspect a deliberate and / or significant violation of this policy is encouraged to promptly report to notifysecurity@bluip.com or call the **BluIP Integrity Line at 855-442-5847** (calls may be made anonymously) or otherwise in accordance with the BluIP Whistleblower Policy. Policy violations will be assessed, and action taken to remediate the violation subject to applicable law and contractual conditions.

Policy Acknowledgment & Review

All individuals subject to this policy:

- complete acknowledgment in BluIP's designated policy management system to confirm you have read, understand, and will follow this policy.
- complete role-specific training based on job function, where applicable.

Acknowledgment & Review Frequency

Personnel review and acknowledge this policy:

- during onboarding or engagement
- annually
- whenever material updates or revisions are made

Compliance Reference: DCF-32

Exception Authority
Exceptions to this policy may be approved by the Chief Executive Officer (CEO) or Chief Operating Officer (COO). All approved exceptions are documented, include a defined duration, and are reviewed periodically.

Roles & Responsibilities

Role	Responsibilities
All Personnel	Understand this policy or seek clarification; avoid activities that expose network systems to unauthorized access or malicious traffic; report suspicious network activity.
Business/Control Owner	Accountable for validating the accuracy of policy content related to their area and manage their team's operational compliance. Maintain business justification for network access supporting their systems, manage team compliance with required network protections, and approve firewall or connectivity needs associated with their applications.
Technical Personnel	Configure, maintain, and monitor Network Security Controls; enforce segmentation, firewall rules, ACLs, and cloud network protections; update documentation (network diagrams, data-flow diagrams) for accuracy; include logging, alerting, and rule reviews occur as required; manage administrative access and change control processes.
Managers & Supervisors	Manage compliance with network security procedures and change control expectations; promote secure network handling practices within their teams.
Vendor / Third-Party	Implement required network protections for systems or services they provide; direct that network security capabilities meet BluIP requirements; notify BluIP of security events or limitations in their logging or monitoring.

System Owner	Maintain knowledge of how their systems connect to and traverse BluIP networks; document, review and approve network rules supporting their system; confirm changes to their system do not bypass Network Security Controls.
Information Security	Provide security guidance, coordinate the policy review process, maintain documentation and evidence, and support compliance with enterprise security standards.
Policy Owner	Update this policy to keep current; comply with the required review and approval processes.
Policy Oversight	Review and approve policy revisions, aligning with governance expectations, regulatory requirements, and risk tolerance.
CEO/COO (Exception Authority)	Approve time-bound policy exceptions and accept associated risk, with periodic review.
Vendor/Third-Party	Provide or support required network protections for services they deliver and manage and notify BluIP of relevant network security events or changes.

Appendix A - Definitions

- **Firewall:** A Network Security Control that controls incoming and outgoing network traffic based on an applied ruleset. A Firewall establishes a barrier between a trusted, secure internal network or host and a network or host that is assumed not to be secure and trusted. Can be physical or virtual.
- **Host Based Firewalls:** Firewalls are designed to protect an individual System regardless of the network that the System is connected to. Host-Based Firewalls are typically provided as an integral component of the host's Operating System (OS) or as a third-party software add-on.
- **Network Perimeter Firewalls*:*** Firewalls located at the boundary between the internal network and external networks such as the Internet. Network Perimeter Firewalls are purpose-built enterprise grade devices (appliances).
- **Network Security Control:** Network policy enforcement points that control network traffic between two or more logical or physical network segments (or subnets) based on predefined policies or rules. BluIP Network Controls include physical firewalls and other cloud access controls and software-defined networking technology.
- **Web Application Firewall:** Controls incoming and outgoing network traffic at layer 7 of the OSI model. A Web Application Firewall examines data content and allows or blocks traffic based on the content of the network connection.
- **Server:** A computing device capable of accepting requests from a client and giving responses accordingly.
- **Systems:** Servers, services, applications or network devices.