Network Security

Policy Intent and Objectives	To protect Paylock resources by defining responsibilities for hardening network components, including intrusion detection systems, firewalls, routers, switches, servers, and creating secure network segmentation as needed to comply with legal, business, client, and regulatory obligations.
Policy Scope	This policy applies to all Paylock personnel, consultants, contractors, vendors, or any other personnel with access to Paylock resources, and covers all Paylock internal computer systems, networks, and electronic communications facilities.
Policy Exceptions	Exceptions to this policy must be documented and approved following Paylock's Exception Procedures.
Policy Enforcement	Violators of this policy are subject to immediate termination of access, and to disciplinary action, as deemed appropriate by Paylock's management. Violators may also be subject to local, state, or federal legal action, depending on the severity of the violation.
Owner	Paul Chiafullo
Approval Date	12-01-2021
Related	Access Control Policy Change Management Process Exceptions Policy Firewall Configuration Standard Information Classification Policy Information Classification Standard Interconnectivity Standard for Clients, Business Partners, and Vendors Logging and Monitoring Policy Network Connectivity Standard Network Connectivity Diagram Standard Remote Access Standard Router Configuration Standard Systems Clock Synchronization Standard

Policy Statements and Guidance	• Network component (e.g., Firewall, Router, and Switch) baseline configuration standards shall be created, maintained, and implemented by the (Paylock to define) department in order to provide a consistent, secure network environment. The standards shall include, but are not limited to:
	  • Disabling unnecessary ports and services;
	  • Eliminating or restricting the use of insecure protocols;
	  • Requiring secure logon and password authentication; and,
	  • Requiring up-to-date documentation comments within the configurations.
	• All vendor-supplied default accounts must be disabled or modified prior to connecting network components to the production network.
	• If hosting providers are utilized, all Paylock policies, procedures, and standards are to be implemented, and all exceptions are to be documented via Paylock's Exceptions Policy. The hosting providers must also meet all Paylock business, legal, and regulatory requirements.
	• Administrative access to network components shall adhere to Paylock's Access Control policy.
	• Non-console access to network components shall take place over secure protocols, and shall utilize encryption per Paylock's Cryptography Policy and Cryptography Standard. All exceptions will require compensating controls and shall be documented via Paylock's Exceptions Policy.
	• Authentication shall be tied to a central authentication resource, such as LDAP. In the event that the central authentication resource is unavailable, access to the network component shall fail closed. A local administrative account can reside on the network component, but the ID and password are to be escrowed for emergency only and must be re-escrowed after each use.
	• Logging shall be turned on and monitored for all network components. These devices are to be actively monitored, and the logs secured from accidental or intentional modification or deletion per the Logging and Monitoring policy.
	• Paylock's IT Security department must review and approve all non-standard Internet connections and must review and validate all private client and vendor connections to/from Paylock corporate network. Non-standard connections include site-to-site VPN.
	• All Internet connections, and all critical network segments, are to be protected by a firewall, and managed by the IT department.
	• The IT Security department must review and approve the purchase of all network components and security devices to ensure it conforms to established security standards.

Policy Statements and Guidance **(continued)**	• All changes to network connections, such as firewalls, routers, and switches, shall be reviewed and approved via the Change Management process. • An alternate remote access solution for clients and business partners may be implemented via a Business-to-Business VPN connection, provided it meets the requirements of Paylock Interconnectivity Standard for Clients, Business Partners, and Vendors. • Insecure protocols, such as Telnet, will require a business justification and must be documented as an exception. Business, legal, security, and regulatory concerns must be addressed prior to approval for an exception. • Updated network diagrams for the Paylock environment shall be maintained by the (Paylock to define) department, and shall be reviewed on a quarterly basis to ensure they are accurate. • Vulnerability scanning of network components shall be managed via the Vulnerability Management Policy. When this is not possible, compensating controls are to be put in place, and the exception documented via Paylock Exceptions Policy. • Network filtering access rules shall be reviewed by the IT department, at a minimum, every six (6) months. These reviews are to be formally documented and retained per business, legal, or regulatory requirements. • Clocks of all network components shall be synchronized to a single reference time source, which shall be documented in the Systems Clock Synchronization Standard. • All information pertaining to network security shall be handled per the Information Classification Policy and the Information Classification Standard.

Policy Revision History	This policy will be reviewed, at a minimum, on an annual basis or as-needed due to legal, regulatory, or corporate directives. The review will include approval by senior management of Paylock prior to any changes being made to the policy.

Date of Policy Change	Description of Policy Change	Change Made By
24 Jul 2017	Creation of policy document	@ Syed Haider
12/01/2021	Policy review - no change	Doreen Gossage
