Endpoint Protection

Policy Intent and Objectives	The intent of this policy is to protect information system and asset integrity and confidentiality by defining requirements for protecting endpoints from malware, data loss, and intrusion.
Policy Scope	This policy applies to all Paylock personnel, consultants, contractors, vendors, or any other personnel with access to Paylock resources.
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	ISO/IEC 27001/27002:2013 – A.12.2 Endpoint Protection Controls Endpoint Protection Standards

Policy Statements and Guidance	• Endpoint protection controls shall be deployed to all servers, workstations, laptops, and any other device (e.g., tablet, phone) where possible.
	• Endpoint protection standards shall be developed to include:
	  • Malware protection.
	  • Intrusion prevention.
	  • Data protection (e.g., encryption).
	  • Logging and monitoring.
	  • A centrally controlled encryption standard for laptops
	  • Physical protection (e.g., cable locks, secure rooms, screen guards).
	• Endpoint protection standards shall define the minimum requirements for specified controls.
	• Paylock support personnel shall be trained on the proper use of malware detection software and how to respond to malware infections and outbreaks.
	• The installation of software on Paylock -owned or -leased information resources by unauthorized personnel is prohibited, unless prior written management approval has been provided through the Exceptions Procedure.
	• Paylock personnel, consultants, contractors, and vendors shall not write, generate, compile, copy, collect, propagate, execute or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of, or access to, any Paylock information resource.
	• Paylock systems users are forbidden from disabling, modifying the settings, or circumventing anti-malware, anti-virus, or other endpoint protection software installed by Paylock.

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
