Vulnerability Management

Policy Intent and Objectives	The intent of this policy is to protect information system and asset availability, integrity, and confidentiality by defining requirements for updating and patching software per Paylock's business, legal, and regulatory requirements.
Policy Scope	This policy applies to all Paylock systems, networks, and applications.
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.12.6 Asset Management Policy Change Management Policy Change Management Process Vulnerability Management Process

Policy Statements and Guidance	• A function shall exist within the Paylock IT department that will have primary responsibility for technical vulnerability monitoring, vulnerability risk assessment, and the updating/patching of vulnerabilities. This resource must have a thorough understanding of vulnerabilities, threats, and risk management of Paylock IT resources. • Vulnerability scanning and the subsequent remediation of such vulnerabilities, required as part of a regulatory obligation shall be managed per the existing regulatory requirement. • To assist in a comprehensive vulnerability management program, a current and complete inventory of information technology assets, over $2,000, shall be kept, including systems/devices, hardware/software vendor, version numbers, deployment location, and custodian of the asset. • Information about technical vulnerabilities of information systems being used shall be obtained from reliable, trusted resources in a timely fashion, the exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk. • Patches are to be tested and evaluated prior to installation to ensure that they will function as intended, and will not introduce side effects that could impact the Paylock production environment. • A vulnerability management standard shall be developed for providing a time frame to address various levels of risk (Critical, High, Medium, Low) that may impact Paylock systems. • In the event that a patch cannot be applied in a timely manner due to technical limitations, or the effect it may have on the production network, compensating controls are to be put in place and documented as an exception. • If a vulnerability has been identified, but a patch or update is not yet available, risk-driven compensating controls are to be put in place until the patch or update is available, tested, and implemented. • Vulnerability patching and updates shall be presented through the Paylock Change Management process for any changes that may affect production processing.

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