

Risk Management Policy

Policy Intent and Objectives	To define the Paylock approach to risk management as it applies to business-critical systems and processes.
Policy Scope	This policy applies to all Paylock business-critical processes, hardware, and software. It also applies to all personnel, consultants, contractors, vendors, or any other human resource performing work for Paylock.
Exceptions	Exceptions to this policy must be documented and approved following Paylock's Exception Procedures.
Enforcement	Violators of this policy are subject to immediate termination of access, and to disciplinary action, as deemed appropriate by Paylock 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 Documents	All Paylock Policies, Procedures, and Standards All Applicable Laws, Regulations, Business Requirements, and Contractual Obligations Paylock Business Impact Analysis (BIA)

Policy Statements and Guidance	<ul style="list-style-type: none"> • Paylock takes a risk-based approach to protect its critical processes, IT infrastructure, proprietary secrets, and critical assets. Risk shall be managed through a combination of preventive, detective, corrective, and compensatory controls. • All critical assets shall be protected, to the most reasonable extent possible, from theft, loss, fraud, manipulation, loss of availability, unauthorized disclosure, or other accidental or malicious acts. • Management shall appoint a Risk Management function within Paylock. The primary responsibility of this function is to identify unacceptable loss by reviewing activities, contracts, programs, or other obligations where the potential for loss is greater than the potential benefits of such arrangements. • A Business Impact Analysis (BIA) shall be performed quarterly, and all critical assets shall be defined, so they can be evaluated against current and reasonably foreseeable threats and vulnerabilities. • Risk profiles of all critical assets are to be reviewed on, at a minimum, an annual basis, with the results of this review submitted to the Paylock Compliance department for review and process documentation. • Any existing asset that, due to business needs, has its status changed to critical must be submitted for a BIA review. Critical assets that will no longer serve such a purpose must also be evaluated and removed from the critical asset list. • Defined critical assets shall be addressed in the Paylock Business Continuity procedure to ensure availability in the event of a business continuity exercise.
---------------------------------------	---

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

