Information Security Organization

Policy Intent and Objectives	The intent of this policy is to establish a management framework to control the implementation and operation of information security within Paylock. The Information Security organization roles and responsibilities are defined by management in support of strategic business goals and objectives.
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.6

Policy Statements and Guidance	• Paylock's Information Security team roles and responsibilities shall include, but are not limited to: • Paylock Security Committee (Members designated from IT, Engineering, Operations, HR and Compliance) • Management and oversight of Paylock's information security posture so that risk, threats, vulnerabilities, and associated costs are managed per Paylock business requirements. • Development, guidance, and management of the information security program to ensure the appropriate controls are in place to monitor for compliance with the objectives of Paylock and its customers. • Providing the appropriate level of technical expertise and support via threat, vulnerability, and risk assessment reviews. • Maintaining an awareness of existing and proposed security policies, procedures, and standards, including state and federal legislation, and regulations pertaining to information security. • Providing information security expertise as part of internal and external meetings when called upon. • Maintaining appropriate contacts with reputable information security special interest groups or other security forums and professional associations. • Participating in project management to ensure that information security risks are identified and addressed as part of project management. • Managing the threat, vulnerability, and risk evaluation process for third parties, vendors, and business partners. • Reviewing processes to make sure the principle of segregation of duties is in place to the greatest extent possible within Paylock. • Verifies that Paylock policies, procedures, and standards are in place during information security reviews. • Maintains the strictest confidentiality and ethics regarding incidents and investigations in which it is asked to participate.

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
