Compliance

Policy Intent and Objectives	The intent of this policy is to ensure that Paylock is in compliance with legislative, regulatory, and contractual requirements affecting information resources.
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.18 Confidentiality Agreement Cryptography Policy Incident Response Procedure Information Classification Policy Information Classification Standard Non-Disclosure Agreement Records Retention Standard

Policy Statements and Guidance	• All relevant legislative statutory, regulatory, contractual requirements and Paylock's approach to meet these requirements shall be identified, documented, and kept up to date by Legal Counsel and delegated to the applicable business unit for implementation and maintenance. • Procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements related to intellectual property rights and the use of proprietary software products (e.g., software licensing, copyright protection). • Records shall be protected from loss, destruction, falsification, unauthorized access, and unauthorized release in accordance with Paylock's Information Classification Policy and the Information Classification Standard, which shall also align with legislative, regulatory, contractual, business, and records retention requirements. • Privacy and protection of personally identifiable information shall be ensured in accordance with Paylock's Information Classification Policy and the Information Classification Standard which shall also align with legislative, regulatory, and contractual requirements. Paylock shall only collect and store the minimum data that is necessary for specified and lawful purposes. • Cryptographic controls shall be used in compliance with all relevant agreements, legislation, and regulations (e.g., import /export laws). • Paylock's approach to managing information security and its implementation (i.e., control objectives, controls, policies, processes, and procedures for information security) shall be reviewed independently at planned intervals, or when significant changes occur. • Directors shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards, and any other security requirements. • Company personnel responsible for collecting personal information should seek to identify the minimum amount of information required in order to properly fulfill the specific business purpose for which it is being collected. • An Incident Response Procedure for all security and privacy-related incidents involving a breach of security of personal information shall be developed and communicated. • Access to any tools (e.g., software, applications, documentation, work papers) required for system audits shall be restricted to authorized individuals.

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	Jennifer Marston
12/01/2021	Policy review - no change	Doreen Gossage