Operations Security and Management

Policy Intent and Objectives	This policy provides guidance on production information resources, routine system operations, virus protection, backup and recovery, and support activities. This policy provides governance to help ensure that confidentiality, integrity, and availability of information resources are maintained.
Policy Scope	This policy applies to all Paylock systems, personnel, third party consultants, contractors, and vendors
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	ISO/IEC 27001/27002:2013 – A12

Policy Statements and Guidance	• Information Technology shall develop, maintain, and make available, documented operating procedures that are used when installing or maintaining information resources • All changes to the organization, business processes, information processing facilities, and systems that affect information security shall adhere to Paylock’s Change Management Process. • Development, test, and production environments shall be separated physically, or at a minimum logically, to reduce the risk of accidental change or unauthorized access to production software and data. • Production data that is classified as sensitive, especially client data, shall not be used in the test or development environments without being scrubbed in order to remove the sensitive data. Substitute data sets will be developed and used for ease of identification as well as testing • Endpoint protection standards shall be developed and deployed to include malware protection, intrusion prevention, and other controls as deemed appropriate based on risk. • Backup facilities and procedures shall be implemented in accordance with Paylock's Backup and Recovery policy • Operations and Management shall utilize the logging and monitoring systems defined in Paylock's Logging and Monitoring policy. • Controls should be implemented to protect against unauthorized changes to log information and monitor for operational problems with the logging facility. • Privileged user account activities shall be logged and regularly reviewed. • Procedures shall be implemented to control the installation of software on operational systems. • Information about technical vulnerabilities shall be communicated in accordance with Paylock's Vulnerability Management policy. • Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to business processes.

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
