Logging and Monitoring

Policy Intent and Objectives	The intent of this policy is to establish requirements for monitoring of information systems to detect and identify security incidents and to meet legal and regulatory requirements.
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.12.4 Event Logging Standards Information Classification Standard Records Retention Standard Systems Clock Synchronization Standard

Policy Statements and Guidance	• Event logging standards shall be developed to define configuration requirements for all information systems, applications, and devices. These standards shall be developed to account for all corporate, legal, and regulatory requirements. • Controls should be defined and implemented to protect against unauthorized changes to log information and to detect log file manipulation by privileged user accounts. • Retention of logging and event data, physical security surveillance, access control, and visitor logs shall be kept for a period of time in accordance with Paylock's corporate, legal, and regulatory requirements. • Privileged user account activities shall be logged and regularly reviewed. • Clocks of all relevant information processing systems shall be synchronized to a single reference time source, which shall be documented in the Systems Clock Synchronization Standard. • Logs that contain sensitive or personally identifiable information shall have appropriate safeguards in place to protect the data. • A capacity management strategy shall be put in place to ensure logs are not overwritten or fail to record log events. • Logging and monitoring data shall be classified per the Information Classification Standard.

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