Information Security Incident Management

Policy Intent and Objectives	The intent of this policy is to establish the requirements for properly managing information security incidents.
Policy Scope	This policy applies to all Paylock personnel, consultants, contractors, vendors, or any other personnel with access to Paylock resources.
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's management. Violators may also be subject to local, state, or federal legal action, depending on the severity of the violation.
Owner	@ Syed Haider aul Chiafullo
Approval Date	12/01/2021
Related Documents	ISO/IEC 27001/27002:2013 – A.16 Confidentiality Agreement Forensic Evidence Handling Procedure Incident Escalation and Communication Procedure Incident Logging Procedure Incident Response Planning and Preparation Process Information Classification Policy Information Classification Standard Monitoring and Detection Process Non-Disclosure Agreement Security Event Standards Security Incident Reporting Procedure

Policy Statements and Guidance	• Incident management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.
	• A point of contact within Paylock shall be established to handle suspected or reported information security incidents.
	• Training shall be provided to ensure only competent personnel handle the issues related to information security incidents within the organization.
	• Only authorized personnel of Paylock may speak to the press or other members of the media regarding information security incidents involving Paylock.
	• Management shall ensure that the following procedures are developed and communicated effectively within the organization, as appropriate:
	  • Process for incident response planning and preparation.
	  • Monitoring, detecting, analyzing, and reporting of information security events and incidents.
	  • Logging incident management activities.
	  • Handling of forensic evidence.
	  • Assessment of, and decision on, information security events and assessment of information security weaknesses.
	  • Process for escalation, controlled recovery from an incident, and communication to internal and external people or organizations as appropriate.
	• Establishment of a point of contact for security incident detection and reporting.
	• Security incident reporting procedures shall include:
	  • Documenting the reporting of information security incidents through a standardized process, and ensuring that Paylock personnel, consultants, contractors, vendors, or anyone with access to Paylock information are aware of and understand the reporting process
	  • The procedure to be followed in case of an information security event, e.g. noting all details immediately, such as type of non-compliance or breach, occurring malfunction, any relevant messages on the screen and immediately reporting to the point of contact, and taking only approved actions.
	  • Reference to an established formal disciplinary process for dealing with employees who commit security breaches.
	  • Once the security incident has been successfully dealt with, a lessons-learned meeting shall be conducted prior to formally closing and recording the security incident.

Policy Statements and Guidance (continued)	• Once the security incident has been successfully dealt with, a retrospective meeting shall be conducted prior to formally closing and recording the security incident (Post Mortem). • All employees and contractors should be made aware of their responsibility to report information security events as quickly as possible. They should also be aware of the procedure for reporting information security events and the point of contact to which the events should be reported. The security incident reporting process should be as easy, accessible, and available as possible. • All incident management data shall be categorized as either Restricted or Confidential, depending on the severity of the incident, per the Information Classification Policy and 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
