Human Resources Security

Policy Intent and Objectives	The intent of the policy is to provide guidance on the necessary procedures and standards for Human Resources so that employees, contractors, and third-party understand their roles and responsibilities in safeguarding Paylock and adhering to Paylock's policies.
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	Teresa Mancini
Approval Date	12-01-2021
Related	ISO/IEC 27001/27002:2013 –A.7 Acceptable Use Policy Anonymous Violation Reporting Procedure Confidentiality Agreement Information Classification Policy Information Classification Standard Non-Disclosure Agreement Pre-Employment Screening Standard

Policy Statements and Guidance	• Paylock Human Resources will manage the employee screening process and associated data. • A Pre-Employment Screening Standard shall be developed to define the investigative checks to be performed on employment candidates, including contractors and temporary staff. • Employees who will be managing sensitive or confidential data processing functions may be subject to additional background checks as dictated by risk, business, or client requirements. • All information collected during the screening process shall be classified as *Confidential,* and protected as defined by the Paylock Information Classification Policy and the Information Classification Standard. • The contractual agreements with employees and contractors shall state all parties' responsibilities for information security. • Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of Paylock. • Paylock shall provide a process to anonymously report violations of security policies or procedures without risk of retribution. • All employees and contractors where relevant to their role shall receive appropriate awareness training and regular updates in organizational policies and procedures, as appropriate for their job function. • There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach with malicious intention. • Confidentiality and non-disclosure agreements shall be defined for any relationship where *Sensitive* or *Confidential* information may be accessed. • An Acceptable Use Policy shall be developed and agreed upon by any individual that accesses or makes use of Paylock's information resources. • A mandatory vacation and personnel rotation standard should be implemented for critical organization roles where the detection and prevention of fraudulent activities warrant it. • Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated, and enforced. • Standards shall be developed and implemented for including security responsibilities in the job descriptions and the performance criteria of personnel who are assigned significant security roles (e.g., security administrators, network security officers, etc.).

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