Supplier Management

Policy Intent and Objectives	The intent of this policy is to address supplier management and to ensure appropriate safeguards are in place to minimize risk to Paylock and its business partners.
Policy Scope	This policy applies to all Paylock service providers (e.g., consultants, contractors, vendors) 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	Doreen Gossage
Approval Date	12/01/2021
Related	ISO/IEC 27001/27002:2013 –A.15 Confidentiality Agreement Information Classification Policy Information Classification Standard Information Security Organization Policy Non-Disclosure Agreement Risk Assessment Questionnaire

Policy Statements and Guidance

- An analysis of any service being outsourced should be completed by the Business Unit interested in establishing the outsourcing agreement. This analysis should document the strategic role and objectives for the outsourcing arrangement. All business units affected by the outsourcing arrangement, or responsible for supporting or maintaining any aspect of the service arrangement, should be consulted and notified during the analysis period.
- For services deemed critical, Paylock must request a review of the service provider's security control practices, business continuity and disaster recovery planning programs.
- All service providers that provide a critical service, or may have access to or otherwise obtain confidential Paylock information, must complete a Paylock Risk Assessment Questionnaire (RAQ).
- The RAQ must be sent to the service provider by the service provider relationship manager and returned to the Information Security Department within an agreed-upon timeline for evaluation.
- Service provider contract reviews shall include the Information Security Department if there are information security sections included within the contract, addendums, or appendices.
- Service provider selection criteria shall include, but is not limited to:
    - A service provider's dependence on other third party providers.
    - For services deemed critical, background checks may be performed for all personnel that would be involved in the service provider arrangement
    - If the service relates to outsourced application development, then code development testing and escrow should also be evaluated.
    - The implications of off-shoring as related to legal and regulatory obligations.
- The following general terms shall be included in agreements with service providers as deemed appropriate by Paylock:
    - A "right to audit" clause reserving Paylock's right to have employees or authorized representatives physically or logically evaluate a third-party service provider's security control environment.
    - Require the third party to immediately inform Paylock of any known or suspected data breaches, or violations of Paylock's Information Security Policies.
    - Require third-party service providers to sign non-disclosure agreements and/or confidentiality agreements.
    - Service Level Agreements (SLAs) for services provided that meet Paylock's operational criteria.
    - Require the 3rd party to hold Paylock harmless for damage done to their systems.
- A regular review process for service level agreements and contracts with third-party service providers shall take place on an annual basis.

Policy Statements and Guidance (continued)	• Any supplier with access to Paylock data shall be contractually obligated to protect Paylock data per the Information Classification Policy and the Information Classification Standard. • Suppliers who discover a breach involving Paylock data shall be contractually required to contact the Paylock relationship manager as soon as possible, no later than 24 hours of the breach discovery, and will make all reasonable efforts to share information regarding how the breach took place, what information is at risk, and what compensating controls were put in place since the breach to contain it. • Suppliers must carry the appropriate amount of insurance in relation to the services provided to Paylock, with the supplier providing verification of such insurance.

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