Change Management Policy

Policy Intent and Objectives	The intent of this policy is to protect information system and asset availability, integrity, and confidentiality by defining requirements for controlling change through documentation, risk assessment, and approval.
Policy Scope	This policy applies to all Paylock information systems
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. Business partners or vendors in violation of this policy may be subject to termination of contract, 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 - A12.1.2 Processes (change management form) Quarterly Patch/Reboot Schedule Actions to take before purposely taking servers offline

Policy Statements and Guidance	• A Change Management Process shall be developed and shall include an assessment of risk associated with a change, testing, an approval process, documentation, notification, backout plans, and appropriate separation of duties. • A Change Advisory Board (CAB) shall be defined and shall meet on a regular basis. The CAB shall have at least one representative from every department, and shall include business unit representation as needed. • Emergency changes shall be approved by the CAB. • All changes, save for pre-approved changes, to information systems, shall adhere to the approved Change Management Process. • Re-tries of changes that were unsuccessful, will require re-approval. • Failed changes with business impact will require a post-mortem. • Any changes that impact clients will be communicated to them with as much advanced notice as possible. • All change management activities must be logged, with a change management form, and maintained for any changes to critical systems. These logs shall be kept per the Paylock Records Retention standard or per regulatory or legal requirements (whichever is greater). • Business own software releases

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