ARYA FIN-TRADE SERVICES (INDIA) PRIVATE LIMITED

CHANGE MANAGEMENT & PATCH MANAGEMENT POLICY

Version	**2024/01.02**
Review Date	**05/04/2024**
Review & Approved by	**Reviewed by Technology Committee & Approved by Board of Directors**

INTRODUCTION

The Information Resources infrastructure at stock brokers' end is expanding and continuously becoming more complex. There are more people dependent upon the network, more client machines, upgraded and expanded administrative systems, and more application programs. As the interdependency between Information Resources infrastructure grows, the need for a strong change management process is essential.

From time to time each Information Resource element requires an outage for planned upgrades, maintenance or fine-tuning. Additionally, unplanned outages may occur that may result in upgrades, maintenance or fine-tuning.

Managing these changes is a critical part of providing a robust and valuable Information Resources infrastructure

1. Purpose

1.1 The purpose of the Change Management Policy is to manage changes in a rational and predictable manner so that staff and clients can plan accordingly. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce negative impact to the user community and to increase the value of Information Resources.

2. Audience

2.1 Change Management Policy applies to all individuals that install, operate or maintain Information Resources.

3. Change Management Policy

3.1 Every change to a Information Resources resource such as: operating systems, computing hardware, networks, and applications is subject to the Change Management Policy and must follow the Change Management Procedures.

3.2 Company has established a scheduled maintenance window that occurs between 4am and 7am on Fridays. All changes affecting user connectivity and access to information resource services must be scheduled within this time frame unless otherwise scheduled with upper management of the Computer Information Systems department.

3.3 All changes affecting computing environmental facilities (e.g., air-conditioning, water, heat, plumbing, electricity, and alarms) need to be reported to or coordinated with the leader of the change management process.

3.4 A Change Management Committee, appointed by designated person, will meet regularly to review change requests and to ensure that change reviews and communications are being satisfactorily performed.

3.5 A formal written change request must be submitted for all changes, both scheduled and unscheduled.

3.6 All scheduled change requests must be submitted in accordance with change management procedures with 2 weeks of prior notice so that the Network Services Department has time to review the request, determine and review potential failures, and make the decision to allow or delay the request.

3.7 Each scheduled change request must receive formal Network Services Department approval before proceeding with the change.

3.8 The appointed leader of the Network Services Department may deny a scheduled or unscheduled change for reasons including, but not limited to, inadequate planning, inadequate back-out plans, the timing of the change will negatively impact a key business process such as year end accounting, or if adequate resources cannot be readily available. Adequate resources may be a problem on weekends, holidays, or during special events.

3.9 Customer notification must be completed for each scheduled or unscheduled change following the steps contained in the Change Management Procedures.

3.10 A Change Review must be completed for each change, whether scheduled or unscheduled, and whether successful or not.

3.11 A Change Management Log must be maintained for all changes. The log must contain, but is not limited to:

3.11.1 Date of submission and date of change

3.11.2 Owner and custodian contact information
3.11.3 Nature of the change
3.11.4 Indication of success or failure signed by all parties involved.
3.11.5 Copies of original files such as
3.12 All information systems must comply with an Information Resources change management process that meets the standards outlined above.
3.13 Violations of this policy must be reported to the Designated Person.

4. Software Patch Management Policy

Introduction

4.1 The Patch Management Policy is designed to ensure the timely and effective application of software patches and updates to information systems in order to mitigate security vulnerabilities, improve system performance, and maintain the overall integrity of the information resources infrastructure.
4.2 This policy applies to all individuals involved in installing, operating, or maintaining information systems within the organization.

5. Patch Management Policy

5.1 A centralized patch management process will be implemented to oversee the identification, testing, deployment, and monitoring of software patches and updates.
5.2 The process will include the following key steps:
5.2.1 Patch Identification:
Regularly monitor vendor releases and security bulletins to identify patches and updates relevant to the organization's information systems.
5.2.2 Patch Testing:
Test patches and updates in a controlled environment before deployment to ensure compatibility, stability, and minimal disruption to the information resources infrastructure.
5.2.3 Patch Deployment:
Develop a deployment strategy to ensure patches and updates are applied promptly and efficiently across all relevant systems while minimizing the impact on users and critical business processes.
5.2.4 Patch Monitoring:
Implement mechanisms to monitor and track the status of applied patches, ensuring their effectiveness and identifying any issues that may require further action.
5.2.5 Patch Documentation:
Maintain accurate and up-to-date documentation of all patch management activities, including patch version details, deployment dates, testing results, and any associated issues or remediation actions taken.
5.3 Compliance with the Patch Management Policy is mandatory for all information systems within the organization.

6. Trading Software Modification

Further in case of trading software modification testing shall be done as per exchange prescribed guideline in Test Environment and/or Mock/Simulation Environment and testing certificate as prescribed by exchange to be obtained and prior approval to be obtained from exchange before live implementation.

7. Disciplinary Actions

7.1 Suitable disciplinary actions shall be taken against employees violating either the Change Management Policy or the Patch Management Policy. These actions will be determined based on the severity and impact of the violation, following the organization's disciplinary procedures and guidelines.