Besseggen Change Management Policy

Doc: Version: 1.2

Document Classification: Internal

Document Control

Document Name	Besseggen Change Management Policy
Abstract	This document describes the Change Management policy at Besseggen Infotech LLP.
Security Classification	Internal
Location	SECTOR-94, NOIDA, GAUTAM BUDH NAGAR-201301

Authorization		
Document Owner	Reviewed by	Authorised by
IT Team	Head – IT	Head – IT

Amendment Log				
Version	Modification Date	Section	A/M/D	Brief description of change
1.1	8 APR 2022	ALL	A	Final
1.2	21 APR 2022	5	M	Reviewed

Distribution list
Chief Information Security Officer (CISO)

ADDRESS: OFFICE NO 1115, ASTRALIS SUPERNOVA PLOT NO 3, FLOOR NO 11, SECTOR 94 NOIDA GAUTAM BUDH NAGAR-201301, UTTAR PRADESH, INDIA, 201301, LLP IDENTIFICATION NUMBER: AAM-6165 (2018-19)

Auditors (Internal & External)
All users,committee at Besseggen Infotech LLP.

TABLE OF CONTENTS

ADDRESS: OFFICE NO 1115, ASTRALIS SUPERNOVA PLOT NO 3, FLOOR NO 11, SECTOR 94 NOIDA GAUTAM BUDH NAGAR-201301, UTTAR PRADESH, INDIA, 201301, LLP IDENTIFICATION NUMBER: AAM-6165 (2018-19)

1. Purpose

Changes to Besseggen Infotech IT facilities and systems shall be controlled in order to ensure that changes made to a production component are applied in a controlled and consistent manner.

2. Scope

This policy applies to all employees, contractors, consultants, and temporary staff etc. using Besseggen Infotech's computing resources. All are expected to be familiar with and comply with this policy.

3. Policy Statement

The change management policy applies to all changes in the following areas:

- Changes to operating systems, which shall include application of patches and service packs, configuration changes, and version upgrades.
- Changes to networks and network devices like routers, switches, firewalls (access control list), etc. This shall include changes to router and switch configurations, firewall policy changes, network layout / traffic changes and changes to intrusion detection systems.
- Changes to IT hardware such as change of RAM, addition / removal of disk drives (HDD, FDD, and CD / DVD Drive) etc.
- Changes in source code
- Additions of new location / new application / new hardware to the existing setup
- Changes to code in the application software being carried out by using proper version controls or special version control software

ADDRESS: OFFICE NO 1115, ASTRALIS SUPERNOVA PLOT NO 3, FLOOR NO 11, SECTOR 94 NOIDA GAUTAM BUDH NAGAR-201301, UTTAR PRADESH, INDIA, 201301, LLP IDENTIFICATION NUMBER: AAM-6165 (2018-19)

4. Responsibility for Policy

The HEAD – IT is responsible for development, maintenance, implementation, operation and escalation of enforcement of these policies and standards.

5. Procedures

5.1 Change Management and Documentation

- The change management process shall involve documenting and managing the change requests.
- The documentation shall provide a brief description of the change requested, the date on which the request was made, priority of the request, tracking and controlling modifications and a unique number for each request.
- All changes shall be planned, scheduled and all the affected parties shall be informed in advance of the change.
- All the Change Request Forms (CRF) should accompany rollback procedures along with them and all changes have to be reviewed after the roll out.

5.2 Change Approval

- Any change request shall be approved by the concerned LOB Head, Application Owner and IT Team based on business requirements or rejected and more clarifications shall be asked from the end user. This request shall be forwarded or acted upon by the relevant team.
- An assessment of the proposed system changes shall be performed to assess its potential impact on Besseggen Infotech's computing systems before its approval.

5.3 Testing of Changes and Backup

- All critical and complex changes shall be tested before being carried out in the live / production environment.

ADDRESS: OFFICE NO 1115, ASTRALIS SUPERNOVA PLOT NO 3, FLOOR NO 11, SECTOR 94 NOIDA GAUTAM BUDH NAGAR-201301, UTTAR PRADESH, INDIA, 201301, LLP IDENTIFICATION NUMBER: AAM-6165 (2018-19)

- A quality assurance test (i.e. including Business Requirement Specification Sign off / Business Solution Group Sign off Process / UAT Sign Off) of the changes shall be performed in a test environment prior to implementation in the production environment.
- A backup of the system impacted by the change shall be made prior to its being updated.
- In case of unsuccessful changes, the rollback and recovery procedures shall be followed.

5.4 Unscheduled / Emergency Changes

- Unscheduled / emergency changes shall be carried out only in case there are critical production issues, which require the change to be carried out.
- Any unscheduled changes shall not be done without proper approval by IT and the concerned LOB Head.
- An audit trail of the emergency activity shall also be generated which logs all activity, including but not limited to:
- The user-ID making the change
- Time and date
- The commands executed
- The program and data files affected
- After unscheduled changes are carried out, normal change procedures shall be expedited.

5.5 User ID and Access Changes

- Any changes to user id including changes to the authorization levels shall be done by following the procedure defined in User Management and Access Control Policy by the approval from IT.
- The change shall involve raising a request and approval of the same by LoB Head of the person requesting access.

5.6 Hardware Changes

- Any changes to hardware shall be done by following the change management process which includes raising a change request,

ADDRESS: OFFICE NO 1115, ASTRALIS SUPERNOVA PLOT NO 3, FLOOR NO 11, SECTOR 94 NOIDA GAUTAM BUDH NAGAR-201301, UTTAR PRADESH, INDIA, 201301, LLP IDENTIFICATION NUMBER: AAM-6165 (2018-19)

approval by the appropriate person and documentation of the same.

- The custodian of the hardware shall conduct all the hardware changes after due approval of the change.
- Changes done to the hardware shall be updated in the hardware / asset register after the change is done.
- Changes done to the hardware shall be monitored after the change to ensure that there is no untoward effect due to the change.

5.7 Operation System and Application Changes

- Any change to the operating system or application shall be strictly controlled by the use of the change management process, which will include raising a change request, testing, approval only by the Head - IT and documentation of the same.
- Changes to the operating system or the application shall be done by following the steps mentioned in the documented operating procedures, wherever applicable.
- All changes shall be documented and a trail must be maintained by means of preserving the change requests for applications.
- Any change that involves downtime or disruption of services shall be done after giving an appropriate notification to the affected users by email.

5.8 Patch and Service Pack Management

- Application of patches shall be done in a controlled manner.
- A patch or service pack shall be applied only when it is a critical patch or there is a requirement for the application of the same.
- Only tested versions of the patch or service pack shall be considered for application, wherever needed.
- The patch or service pack shall be obtained directly from the vendor or downloaded from the vendor site only.
- A test bed shall be prepared whenever possible to simulate the actual production environment and the patch or service pack shall be installed in the test environment. The test environment shall be monitored for performance and other issues.
- On successful testing by the functional users on the UAT server, the

ADDRESS: OFFICE NO 1115, ASTRALIS SUPERNOVA PLOT NO 3, FLOOR NO 11, SECTOR 94 NOIDA GAUTAM BUDH NAGAR-201301, UTTAR PRADESH, INDIA, 201301, LLP IDENTIFICATION NUMBER: AAM-6165 (2018-19)

patch shall be applied on the production server.

- Patching and auto-update process for desktops / laptops has been omitted from the change management process considering the low / negligible business impact. Patches to the desktops / laptops can be applied directly by using the auto-update feature.

5.9 Source Code Management

- A repository for production source code shall be maintained for critical servers. Developers shall retrieve the source code from this repository when modifying programs. Only authorized developers shall have access to the repository.
- A backup copy of the source code shall be properly safeguarded by the development team / vendor.
- Source codes shall be maintained with proper version control.

5.10 Changes in production environment

- Addition, removal of any hardware, software or IT resource from the production environment shall be controlled and approved and a complete track shall be maintained to ensure non-disruption of the production environment.

6. Enforcement

Any user found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, or legal action as appropriate, or both. No provision of this policy will alter the at-will nature of the employment relationship at Besseggen Infotech.

7. References

Change Request Form

ADDRESS: OFFICE NO 1115, ASTRALIS SUPERNOVA PLOT NO 3, FLOOR NO 11, SECTOR 94 NOIDA GAUTAM BUDH NAGAR-201301, UTTAR PRADESH, INDIA, 201301, LLP IDENTIFICATION NUMBER: AAM-6165 (2018-19)