Besseggen User Management and Access Control Policy

Doc: Version: 1.3

Document Classification: Internal

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)

Document Control

Document Name	Besseggen User Management and Access control Policy
Abstract	This document describes the User Management and Access control 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	18 APR 2022	ALL	A	Final
1.2	20 APR 2022	3,5	M	Reviewed
1.3	20 Oct 2023	ALL		Reviewed

Distribution list

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)

Chief Information Security Officer (CISO)
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

The purpose of this policy is to prevent unauthorized access to the Besseggen Infotech information systems. The policy describes the registration and de-registration process for all Besseggen Infotech information systems and services.

2. Scope

This policy applies to all Besseggen Infotech employees, consultants who are a new starter, leaver, moving job, responsibility or Portfolio.

3. Policy Statement

3.1 Managing User Access

- Besseggen Infotech users shall be granted access to information, data and applications strictly on a "need to know" basis.
- Any change in access privileges shall be carried out only after approved by appropriate personnel, by using a formal documented process.
- Segregation of duties shall exist between information access requestors, information access approvers and those implementing

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)

access changes. Each of these roles is limited to a pre-defined group and only those specifically given the responsibility shall be allowed to either request or approve access.

- All access changes shall be carried by the IT Team specifically authorized to carry out such changes. Examples of access changes include: creation of new employee accounts, transfers, terminations, file folder permissions, etc.
- User access rights to applications and data shall be assigned only by the application administrator, on receipt of a documented approval from the LoB Head of the person requesting access. All access requests shall include the purpose for request of access.
- If for any reason, a user's access rights need to be modified or revoked, the LoB Head shall send the request for the same in writing to the IT Team. The IT Team shall then accordingly modify / revoke the access rights. If the same change is for an application then the LoB Head shall send the request to the application administrator.
- HR shall promptly report all changes (i.e. LoB transfers, termination, job duty changes) in end-user duties or employment status to the IT Team handling the user IDs of the affected persons. The IT Team shall then accordingly modify / revoke the access rights. If the same change is for an application then the HR shall send the request to the application administrator.
- All users shall be granted "read" access to all information classified as "public". Other rights to such information shall be strictly reserved with the owner of such information.

3.1.1 Access Logs

Access logs shall be monitored and reviewed on a defined period. A reactive approach shall be adopted for log review where incidents shall be analyzed only when reported / requested and report shall be submitted to the HEAD – IT.

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)

3.1.2 Managing User Id

User Ids shall follow a standard naming convention for all computer systems to facilitate user identification. Naming conventions will cover all end users, contractors, consultants and vendors. Generic IDs shall not be used.

- Access to information services shall be controlled by using unique user Ids, wherever possible, which will enable:
- individual accountability
- permit centralized identification of users
- aids in timely control of potential threats
- "Guest" accounts and other default accounts shall be disabled on all servers.
- Each user is personally responsible for the usage of his or her user ID and password

3.1.3 Password Management

- An initial password shall be provided to the users in a secure manner during the user creation process and the system shall be configured to force the users to change the initial password immediately after the first logon.
- Passwords shall be conveyed to users in a secure manner. Passwords shall never be disclosed via telephone or through third parties or through unprotected (clear text) electronic mails.
- Password constraints and account policy shall be enforced for all user and administrator accounts on operating systems, applications, databases and all other information protected by password controls. The controls enforced shall be as per Password Policy.
- Due to system limitations or business necessity, if any of the password policy cannot be followed, associated risk should be

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)

brought to the attention of the management, and exceptions shall be documented. Compensating controls shall be put in place to mitigate the associated risk.

3.2 Ensuring Logical Security on Laptops and Desktops

- The folders or disk drives in individual desktops or laptops shall not be shared unless appropriate access controls have been enabled on the folder or the disk drive. Sharing of any information classified as 'restricted' or 'confidential' is not permitted unless authorized by concerned authority.
- If any removable devices like pen drives, CD Writer etc. need to be used their prior approval shall be taken from the LoB head.

3.3 Ensuring Physical Security of Laptops and Desktops, Docs, Intellectual Properties

- Users at Besseggen Infotech should ensure physical security of devices and documents.
- Clear desk and clear screen policy should be adopted when such devices or docs are not in use.

3.4 Controlling Privileged User IDs

Use of privileged user IDs

- User ids with high-level access privileges (administrators) shall only be used in the event of emergency.
- System Administrator shall logon using their normal user Id when performing regular work duties rather than logging in as 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)

administrator. Use of Administrator profile shall be limited to administrative activities only.

- Passwords of such user Ids shall be stored in sealed envelopes in the company safe. This will ensure that an authorized employee has access to this password, in the event that the concerned person cannot be reached during an emergency.
- All emergency actions, which bypass normal access control procedures, shall be logged and reported for immediate review by delegated authority.

Usage of Sensitive System Utilities

- Sensitive system utilities are the utilities which give unrestricted access to the critical system resources. The sensitive system utilities include but are not limited to Format, User addition / deletion / update, Change in Network Settings.

Restricting Use of System Utilities

- Access to system utilities shall be restricted to authorized personnel in accordance with their business functions and business needs.
- All unnecessary sensitive utilities shall be removed / disabled from the system.
- The use of all system utilities shall be logged and regularly reviewed by the IT Team.
- It shall be ensured that normal users do not have access rights to use utilities.
- System utilities shall be separated from application 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 Access Control

This access control process is to be followed for the following areas:

- Network (LAN) access
- Internet access
- Application access
- Access card

For new joinees the HR department shall inform the IT Team for creation of username/password for Active Directory. The details shall be sent to the new joinees in a secure manner. The new joinees should be forced to change the password on first use.

Access Approval Process

The process for access provision to various IT resources is as below:

- Users must inform the LoB Head, who would approve or reject the request.
- On approval, the request must be forwarded to the IT team who would implement the request.
- The IT Team must do the necessary steps (create id and password, etc.) and inform the initiator of the request.
- In case of application access, the request must be forwarded to 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)

application administrator for further processing.

- The application administrator should keep a record of all the users which have access to the application.

Access Deletion Process

While there is a well-defined process to provide access, it is equally important that account disabling should also follow a well-defined process.

- Wherever possible, the user ids must not be immediately deleted, but kept disabled for a period of one month and then deleted. Disabling of user accounts rather than deleting has the advantage in case of any requirement to perform forensic analysis; the user details will be still available.
- In cases where an account has to be deleted, the user logs and details must be backed up before deleting the account.

In case of disabling:

- IT Team / application administrator would disable the user id and update the user id database with the status of the user id
- In case of email ID, the emails should be forwarded to the designated person by the LoB Head. Appropriate Out of office messages should be set for the disabled email id informing the senders.
- The IT Team / application administrator would inform the initiator of the request.

In case of deletion:

- The IT Team /application administrator should back up all user information, including emails.
- The backup of the user information must be handed over to the concerned person in the related department.
- IT Team /application administrator would delete the user id and update

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)

the user id list with the status of the user id.

- The IT Team /application administrator would inform the initiator of the request.

5.2 User Id Management

The following guidelines must be followed:

- All users must have a unique user id, and it must not be shared between multiple people, unless approved and signed off by LoB Head for some specific business purpose.
- The names of default accounts (like administrator) must be renamed, wherever possible or deleted wherever applicable.

User ID Nomenclature

- The user ID for systems must follow a nomenclature defined and documented in the system documentation for that system.
- The same nomenclature must be followed for all users within that system.

Recording of User Ids

- The user id and the associated privileges of all users within the system must be recorded.
- The system administrators of all systems must create, maintain and manage this list. The format may vary for different applications.

5.3 Password Management

Password Allocation Process

- In order to ensure that passwords are communicated only to 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)

relevant user, they must be communicated back to the originator of the request or the person to whom it is assigned. The initial passwords must be communicated directly in person to the user.

- All initial passwords must be configured to "Force Modify" on the first usage.

Password Reset Process

- Users / administrators during the course of time may forget their passwords, in which case the same has to be reset. If the password reset is not done in a proper and secure manner, it is possible for unauthorized users to ask for passwords of authorized users to be reset and gain access to systems.

5.4 Privileged User ID and Password Management

Privileged User ID maintenance procedures

The following procedures must be maintained for the operation and maintenance of privileged user ids that have got high levels of authorization in critical systems:

- User Ids with special system privileges must be controlled and restricted to a limited number of authorized personnel.
- Privileged user ids must include ids, which are used to administer modifications to the operating system, security functions and audit logs.
- Administrators must logon as themselves, using a normal user Id when performing regular work duties rather than logging in as the Supervisor / Administrator. Logging in as the Supervisor / Administrator must be limited to administrative activities only.
- A list of the privileged user ids that are used for the administration of the critical systems must be maintained.

Privileged Password management procedures

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)

- All critical system passwords must be written on a paper, put in envelopes and stored securely under lock and key.
- These envelopes should be placed in the company safe and in the custody of LoB Head. These passwords shall be used in case of emergency only. Distribution list shall be maintained and signed off.
- The use of the password stored in the envelope must be logged, and the password must be changed immediately after use.

Emergency User ID Management Procedures

- Emergency ids which have high-level access privileges must only be created and used in the event of extreme emergency only.
- All emergency actions, which bypass normal access control procedures, must be logged and reported for immediate review by LoB Head or Head – IT Team.
- Designated owners must be notified immediately of all emergency fixes and they must retrospectively review all emergency amendments to their production environment.

Review of User Access Rights

- User access rights for all critical systems must be reviewed at an interval of 6 months.
- IT Team shall prepare the list of users (Active Directory) and associated privileges for each of the LoB. The IT Team shall send it to the respective LoB Heads for the confirmation. LoB Head shall confirm the privileges and notify any deviations. IT Team shall rectify the deviations notified by the LoB Heads.
- In case the authentication and authorization for an application not being managed by a centralized active directory, then the application administrator managing the system shall prepare the list of application users and associated privileges. The list should be sent to the related LoB Head for the confirmation. LoB Head shall confirm the privileges and notify any deviations. Application administrator shall rectify the deviations notified by the LoB Heads.

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)

- Authorizations for special privileged (Administrative) access rights must be reviewed at an interval of 6 months or earlier on a need basis. HEAD – IT shall review all the accounts with special privileges and notify any deviations to the IT Team for rectification.
- The user access rights must be reviewed when changes to user's normal duties are required, for example, as a result of resignation, termination, transfer or promotion.

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

Access controls for accessing the binaries and executing trades—

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)

Entity	User	Access to Trading Platform Binary	Access to Financial Reports	Modify Trading Algorithms	Execute Trades	Access to Change Mandates
Partner	Vibhu Garg	Full Access	Full Access	Full Access	Full Access	Full Access
	Ankit Pruthi	Full Access	Full Access	Full Access	Full Access	Full Access
	Karun Singla	Full Access	Full Access	Full Access	Full Access	Full Access
Developer	Nishant Agarwal	Limited Access	Limited Access	Limited Access	Limited Access	No Access
	Prince Kumar	Limited Access	Limited Access	Limited Access	Limited Access	No Access
	Shubham Bansal	Limited Access	Limited Access	Limited Access	Limited Access	No Access

Authority matrix —

Entity	User	Sudo	Execute	Read	Write
Partner	Vibhu Garg	Allowed	Allowed	Allowed	Allowed
	Ankit Pruthi	Allowed	Allowed	Allowed	Allowed
	Karun Singla	Allowed	Allowed	Allowed	Allowed

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)

Developer	Nishant Agarwal	Deny	Partially Allowed	Partially Allowed	Partially Allowed
	Prince Kumar	Deny	Partially Allowed	Partially Allowed	Partially Allowed
	Shubham Bansal	Deny	Partially Allowed	Partially Allowed	Partially Allowed

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)