BESSEGGEN INFOTECH LLP

Information and Cyber Security Framework

ROLE BASED ACCESS CONTROL POLICY

Reference No.: BESSEGGEN/I&CSF/ISP&P

Version: 1.1

14th June 2025

Internal Use Only

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			
Reference No.	BESSEGGEN/I&CSF/ISP&P		
Document Name	**Besseggen_role_based_access_control_policy**		
Version No.	1.1		
Document Status	Definitive		
Issue Date	14th June 2025		
Compliance Status	Mandatory		
Review Period	One year from the date of release or earlier if required		
Security Classification	Internal Use Only		
Distribution	Part of BESSEGGEN ISP&P		
	Name	**Role**	**Signature**
Authored by	BESSEGGEN INFOTECH LLP		
Reviewed by	Ankit Pruthi	Partner	
Approved by	Vibhu Garg	CISO & Partner	
Released by	BESSEGGEN INFOTECH LLP		

Document Revision History		
Version	**Release Date**	**Change Description**
1.0	18th July 2024	All added
1.1	14th June 2025	Reviewed

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)

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

This policy establishes rules for granting, modifying, reviewing, and revoking access rights to information systems and resources based on defined roles within NSE/BSE IT and operational infrastructure.

2. Scope

This policy applies to all employees, vendors, contractors, and third-party users who access NSE/BSE information systems and resources.

3. Definitions

- RBAC (Role-Based Access Control): Access control model that restricts system access based on a user's role.
- Role: A job function or responsibility within the organization that defines an authority level.
- Least Privilege: Users are given the minimum levels of access—or permissions—needed to perform their job functions.
- Segregation of Duties (SoD): No single individual should have control over all aspects of any critical process.

4. Roles and Responsibilities

Role	Responsibilities
CISO	Approves access control policies and ensures compliance with ISO 27001
IT Security Team	Manages RBAC implementation, monitoring, and reviews

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)

HR Department	Provides role assignment and change details to IT
System Owners	Approve role-based access for their systems
End Users	Use only authorized access and report anomalies immediately

5. RBAC Implementation Framework

User Role	System / Resource Access	Access Type	Approval Required
Trading Operator	Trading system, market feed	Read/Execute	Department Head
Surveillance Analyst	Surveillance data dashboards	Read-only	Surveillance Head
IT Admin	Servers, user directories, firewall	Full (Admin)	CISO
Developer	Dev/test servers only	Read/Write	IT Manager
Finance Officer	Billing, reporting systems	Read/Write	Finance Head
Auditor	Logs, records (limited view)	Read-only	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)

6. Access Request and Review Process

- All access requests must be submitted via the official Access Request Form.
- Access must be granted only after proper role validation and approval.
- Quarterly reviews of user roles and access rights shall be conducted by the IT Security Team.
- Terminated or transferred users must have access revoked within 24 hours.

7. Policy Enforcement and Exceptions

Any violation of this policy may lead to disciplinary actions. Exceptions must be documented and approved by the CISO.

8. Policy Review and Update

This policy shall be reviewed annually or in case of significant changes in organizational structure, systems, or compliance requirements.

9. Related Documents

Besseggen_ICSF_information_security_policy_&_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)