AHF Smart ERP Policy Document

ERP stands for Enterprise Resource Planning and is a software solution that helps organizations manage their resources, streamline their business processes, and improve their productivity. This is an industry standard term referring to software applications used to operate the business function of an organization (AHF).

It is the operational requirement of AHF to provide, state-of-the-art ERP System and electronic communication services through Internet and intranet to enhance the workflow and carry out the administrative activities to promote effectiveness and efficiency. For this purpose, AHF has established ERP usage policy that outlines the use and controls.

Purpose

The purpose of this policy is to ensure AHF Smart ERP usage is consistent, well understood, managed, secured, effective, and efficient by outlining the procedures and guidelines for using and controlling the system.

Policy Statement – Changes in access to the ERP system will be granted as described below.

i. A request in writing from the supervisor of the requesting employee must detail the access to be given. Official authorised e-mail is the preferred method of communication for this purpose.

ii. The request should list access levels, file, and site (cost center) to which the employee should be granted access. In the event a security access class already exists either for an existing employee or from the employee previously holding the position, it is acceptable to reference that in lieu of a detailed list of each access levels, file, and site (cost center).

Scope

This policy applies to all employees, contractors, and third-party service providers who access the ERP system or data from AHF departments.

Workflow Review and Approval

All workflows running the ERP are implemented in line with AHF policy, reviewed and approved by Bureau Chief before implementation in the live environment.

Roles and Responsibilities

All authorized users are provided with a username and password to login into the ERP and access the required features. Each user has features defined as per the departmental job role and requirement.

User roles and permissions are clearly defined, granting access privileges based on job responsibilities and ensuring segregation of duties to prevent collusion and unauthorized access to critical functions like financial transactions or master data changes.

a. IT Department: The IT department is responsible for maintaining the ERP system and ensuring, it is up-to-date and secure. The IT department also provide training to users and monitors the system for any potential security breaches.

b. ERP System Administrator: The ERP system administrator (IT department) is responsible for managing user access, setting up user accounts, and ensuring users have the appropriate access permissions.
c. Users: Users include person / stakeholders assigned roles in the system and responsible for using the AHF Smart ERP in accordance with this policy and any additional guidelines provided by the Management through IT department.

User Access

User access and access controls are granted by IT department after approvals from respective department heads, ensuring only authorized personnel have access to sensitive financial and operational data stored in the ERP system.

a. User accounts: User accounts will be created and managed by the ERP system administrator. Users will be assigned the appropriate level of access based on their job duties.
b. Passwords: Users must select a strong password and change it every 90 days. Passwords must not be shared with others and should be kept confidential. The password should have a combination of uppercase letters, lowercase letters, numbers, and symbols.
c. User Access Reviews: User access will be reviewed annually to ensure that users have the appropriate level of access based on their job duties or as directed by the country leads.

Data Security

a. Data Classification: All data in the ERP system should be classified based on its sensitivity. Users should only access data that is required for their job duties.
b. Data Backups: Daily backups of the ERP system data should be taken to ensure that data is not lost in the event of a system failure.
c. Security Incidents: Any security incidents involving the ERP system must be reported to the IT department immediately.

Misuse of Data

Misuse of the ERP System would cover every action that disturbs the use of System for the purpose it is meant for. Causing harm or damage in any data, using characteristics of the systems for purposes that they are not meant for is prohibited by the administrators of the ERP systems.

Misuse of the ERP may constitute a criminal activity or may constitute abuse of office, including (but not limited to) the following:

i. Alteration of data without authorization.
ii. Information classified as confidential or proprietary must not be sent over the Internet, for example: a file transfer, email content, file attachment or via a web session, unless protected by appropriate security measures.
iii. Unauthorized access to or use of other users' accounts.
iv. Unauthorized decryption of coded information such as passwords.
v. Forgery or attempted forgery of data.

vi. Intentionally introducing ~~of~~ viruses or other disruptive/ destructive programs that affect the normal operation of the ERP.

vii. Attempts to evade or bypass system administration policies, such as resource quotas, firewall and web filter settings.

viii. Uploading or downloading any kind of socially or ethically objectionable material.

Fraud Prevention

a. Any form of fraudulent activity, including but not limited to embezzlement, misappropriation of funds, or manipulation of financial data, is strictly prohibited within the AHF Smart ERP system.

b. Participation in fraudulent activities will result in disciplinary actions, including termination of employment and potential legal action.

c. You must report any suspected or observed fraudulent activities to the appropriate authorities or designated individuals within the organization as below: -

  - the CPD/Ms,
  - Regional Finance Team
  - Regional IT team
  - Regional Security team

d. Regular communication will be done to inform employees about new fraud trends, reporting mechanisms, and the consequences of fraudulent actions.

Data Integrity and Validation

a. When using the system, data integrity is a priority to maintain accurate and reliable data within the Smart ERP system to prevent fraudulent activities.

b. Regular data validation and integrity checks will be conducted to identify and rectify any discrepancies, reducing the risk of fraudulent manipulation of data.

Monitoring and Auditing

a. The ERP system is continuously monitored, and audits will be done periodically to detect any irregularities or anomalies that may indicate fraudulent activities.

b. System logs, audit trails, and exception reporting mechanisms are used to identify any suspicious transactions or unauthorized access attempts.

Whistleblower Protection:

a. There is guaranteed protection to any employee who reports suspected fraud in good faith from retaliation or adverse consequences and all information will be treated confidential as per the HR whistleblower policy and procedures.

b. Alternative reporting channels, such as anonymous hotlines or confidential email addresses to security department is a safe and secure way to report concerns.

Training

All users must complete ERP system training before accessing the system. Additional training may be required based on changes to the system or job duties / roles.

Ongoing training and awareness programs will be conducted to educate employees about the risks of fraud within the ERP system.

Compliance

All users must comply with this policy and any additional guidelines provided by the IT department. Failure to comply may result to account deactivation.

Review and Revision

This policy will be reviewed annually by the IT department and revised as needed to ensure it remains effective and up to date with changes to the organization or technology.

Conclusion

This policy provides guidelines for the effective and secure use of ERP within AHF countries. By following these guidelines, we can ensure our resources are used efficiently and effectively, and that our operational processes are streamlined to meet the needs of AHF.