FUJIYAMA POWER SYSTEMS LIMITED

Access Management Procedure

1. Objective

To ensure that user access to **BUSY Accounting Software** is granted, modified, reviewed, and revoked in a controlled manner to prevent unauthorized access and maintain data integrity.

2. Scope

This procedure applies to:

- All users of BUSY software (employees, contract staff, third parties)
- All BUSY modules including Accounting, Inventory, GST, Payroll, and Reports

3. Roles & Responsibilities

- **User / Department Head**: Requests and approves access based on job responsibility
- **IT Department**: Creates, modifies, and deactivates BUSY user IDs
- **HR Department**: Intimates IT regarding employee joining, role change, or exit
- **Internal Auditor**: Periodically reviews access controls and compliance

4. User Access Provisioning

- Access to BUSY shall be provided only upon **approved access request**.
- User access shall be **role-based** and limited to business requirements.
- User IDs in BUSY shall be created **only by the IT Department**.
- Initial passwords shall be set by IT and shared securely.
- Users are required to change passwords at first login (where system allows).

5. Access Rights Configuration (BUSY Specific)

- Access rights such as **Voucher Entry, Modification, Deletion, Reports, Masters, and GST Returns** shall be granted as per role.
- Critical rights (e.g., voucher deletion, backdated entries, master modification) shall be restricted and approved by management.

6. Access Modification

- Any change in role or responsibility shall require revised approval.
- IT shall update BUSY access rights only after receiving documented authorization.

7. Access Revocation (Employee Exit)

- HR shall inform IT immediately upon employee resignation, termination, or transfer.
- IT shall deactivate BUSY user ID on or before the **last working day**.
- Access of inactive users shall be periodically reviewed and disabled.

8. Periodic Access Review

- BUSY user access rights shall be reviewed **at least annually / quarterly**.
- Excess or unauthorized access, if identified, shall be removed immediately.

9. Third-Party Access

- Third-party or consultant access to BUSY shall be:
  - Time-bound
  - Approved by management
  - Revoked immediately after work completion

10. Logging and Monitoring

- Where feasible, BUSY audit logs, user activity, and changes in masters/vouchers shall be reviewed periodically.
- Any unusual or unauthorized activity shall be investigated.

11. Non-Compliance

Non-compliance with this procedure may lead to disciplinary action and shall be reported to management.

FUJIYAMA POWER SYSTEMS LIMITED

Data Backup and Restoration Policy

1. Objective

To ensure that critical business data and systems are backed up regularly and can be restored in a timely manner in case of data loss, system failure, or security incidents.

2. Scope

This policy applies to:

- All critical IT systems and applications, including **BUSY accounting software**
- Financial, accounting, inventory, GST, and operational data
- Servers, desktops, laptops, and storage devices used for business purposes

3. Roles & Responsibilities

- **IT Department**: Perform, monitor, and document backup and restoration activities
- **System Users**: Ensure business data is saved in designated locations
- **Management**: Review critical restoration activities
- **Internal Auditor**: Periodically review compliance with this policy

4. Data Backup

- **Daily Backup**: BUSY data and other critical financial data
- **Weekly Backup**: Full system or database backup (where feasible)
- **Monthly Backup**: Archival backup for record retention

(Backup frequency may vary based on system criticality and technical feasibility.)

5. Backup Storage & Security

- Backup data shall be stored in secure locations such as external hard drives, network storage, or cloud storage.
- At least one copy of backup data shall be stored in an off-site or separate secured location.
- Access to backup data shall be restricted to authorized IT personnel only.
- Backup data shall be protected against unauthorized access, alteration, or deletion.

6. Backup Verification

- IT shall periodically verify successful completion of backups.
- Any backup failure shall be investigated and resolved promptly.

7. Data Restoration

- Data restoration shall be performed only upon authorization from IT and relevant management.
- Restoration may be initiated in case of:
    - Data loss or corruption
    - System failure
    - Security incident
    - Accidental deletion or processing errors
- Restoration activities shall be documented, including reason, date, and data restored.

8. Restoration Testing

- Periodic restoration testing shall be performed to ensure data recoverability.
- Evidence of successful restoration testing shall be maintained.

9. Backup Retention

- Backup data shall be retained as per statutory and business requirements.
- Obsolete backups shall be disposed of securely.

10. Third-Party Backup & Restoration

- Where backup or restoration activities are handled by third-party service providers, adequate controls and approvals shall be ensured.
- Third-party access shall be time-bound and monitored.

11. Incident Handling

- Backup and restoration activities arising due to incidents shall be aligned with the **Incident Management Policy**.
- All restoration activities shall be reviewed for root cause and preventive actions.

12. Compliance

Non-compliance with this policy may result in disciplinary action and may attract legal consequences.

13. Policy Review

This policy shall be reviewed periodically and updated as required.

FUJIYAMA POWER SYSTEMS LIMITED

Business Continuity and Disaster Recovery Policy

1. Objective

To ensure continuity of critical business operations and timely recovery of IT systems and data in the event of disruptions such as system failure, data loss, cyber incidents, or natural disasters.

2. Scope

This policy applies to:

- All critical business processes and departments
- All IT systems and applications, including **BUSY accounting software**
- Employees, contractual staff, and third-party service providers

3. Business Continuity & Disaster Events

Events covered under this policy include, but are not limited to:

- System or server failure
- Data corruption or cyber security incidents
- Power outage or network failure
- Fire, flood, earthquake, or other natural disasters
- Pandemic or manpower unavailability
- Failure of third-party or service providers

4. Roles & Responsibilities

- **Management**: Overall responsibility for BCP & DR readiness
- **IT Department**: System recovery, data restoration, and technical support
- **Department Heads**: Identify critical processes and support continuity actions
- **Employees**: Follow continuity instructions during disruption
- **Internal Auditor**: Periodic review of compliance and effectiveness

5. Critical Business Processes & Systems

- Critical processes include accounting, inventory, GST compliance, payroll, and statutory reporting.
- Critical systems include BUSY ERP and supporting IT infrastructure.
- Priority shall be given to restoring systems impacting financial and regulatory reporting.

6. Business Continuity Measures (BCP)

- Regular data backups shall be maintained as per the **Data Backup and Restoration Policy**.

- Alternate work arrangements (work-from-home, alternate location, or manual processing) shall be adopted where required.
- Key documents and data shall be made accessible during disruptions.

7. Disaster Recovery (DR) Measures

- In case of major system failure or data loss, IT shall restore systems and data using the most recent available backup.
- Restoration activities shall be authorized and documented.
- Recovery efforts shall focus on minimizing downtime and business impact.

8. Communication & Escalation

- Clear communication channels shall be established to inform management and affected users during disruption.
- Critical incidents shall be escalated immediately to senior management.

9. Third-Party & Vendor Continuity

- Dependencies on third-party vendors shall be identified.
- Vendors providing critical services shall be expected to maintain adequate continuity and recovery arrangements.

10. Testing & Review

- BCP & DR arrangements shall be tested periodically through mock drills or tabletop exercises, where feasible.
- Gaps identified during testing shall be addressed appropriately.

11. Training & Awareness

- Employees shall be made aware of basic BCP & DR responsibilities relevant to their roles.

12. Compliance

Non-compliance with this policy may result in disciplinary action and shall be reported to management.

FUJIYAMA POWER SYSTEMS LIMITED

Change Management Policy

1. Objective

To ensure that all changes to IT systems, applications, and configurations are authorized, tested, documented, and implemented in a controlled manner to prevent unauthorized or unintended impact on business operations.

2. Scope

This policy applies to:

- All changes related to IT systems and applications, including **BUSY software**
- Master data changes, configuration changes, patches, upgrades, and report logic changes
- Changes initiated by internal users or third parties

3. Roles & Responsibilities

- **User / Department Head**: Initiates and approves change requests
- **IT Department**: Evaluates, implements, and documents changes
- **Management**: Approves significant or critical changes
- **Internal Auditor**: Reviews compliance with this policy

4. Change Request Initiation

- All changes shall be initiated through a **documented change request** (email / ticket / form).
- The request shall include:
    - Nature of change
    - Reason for change
    - Impact assessment
    - Requested date

5. Change Approval

- Changes shall be approved by the respective Department Head and IT.
- Critical changes (e.g., changes affecting financial data, GST, reports, or controls in BUSY) shall require **management approval** before implementation.

6. Change Testing

- Changes shall be tested in a test environment or validated through sample checks where feasible.
- Evidence of testing shall be documented, especially for critical changes.

7. Change Implementation

- Approved changes shall be implemented by the IT Department only.
- Changes shall be implemented during authorized time windows to minimize business disruption.
- Post-implementation verification shall be performed to ensure correctness.

8. Emergency Changes

- Emergency changes required to restore system operations shall be approved retrospectively.
- Emergency changes shall be documented and reviewed after implementation.

9. Change Documentation & Record Keeping

- All change requests, approvals, testing evidence, and implementation details shall be retained for audit purposes.
- A **change log** shall be maintained by the IT Department.

10. Third-Party Changes

- Changes carried out by third parties (vendors, consultants) shall follow the same approval and documentation process.
- Access provided for changes shall be time-bound and revoked after completion.

11. Compliance & Monitoring

- Non-compliance with this policy shall be reported to management.
- Periodic review of changes shall be conducted as part of internal audit.

FUJIYAMA POWER SYSTEMS LIMITED

Incident Management Policy

1. Objective

To ensure that information security and system incidents are identified, reported, investigated, resolved, and documented in a timely manner to minimize impact on business operations and data integrity.

2. Scope

This policy applies to:

- All IT systems and applications, including **BUSY software**
- All employees, contract staff, and third-party users
- All incidents related to system availability, data security, unauthorized access, malware, and operational disruptions

3. Definition of Incident

An incident includes, but is not limited to:

- Unauthorized system or application access
- Data loss, data leakage, or data corruption
- Malware or virus infection
- System downtime or application failure
- Incorrect system processing impacting financial or operational data
- Security policy violations

4. Roles & Responsibilities

- **Users**: Immediately report any suspected or actual incident
- **IT Department**: Record, analyze, resolve, and document incidents
- **Management**: Review significant or critical incidents
- **Internal Auditor**: Periodically review incident records and compliance

5. Incident Reporting

- All incidents shall be reported immediately to the IT Department via email, ticket, or other defined communication channels.
- The incident report shall include:
    - Date and time of occurrence
    - Nature of incident
    - Systems impacted
    - Initial assessment of impact

6. Incident Classification

Incidents shall be classified based on severity:

- **Low**: No significant business impact
- **Medium**: Temporary disruption or limited data impact
- **High/Critical**: Significant system downtime, financial impact, or data breach

7. Incident Response & Resolution

- IT shall analyze the incident and take corrective actions to contain and resolve it.
- Root cause analysis shall be performed for medium and high incidents.
- Corrective and preventive actions shall be documented.

8. Incident Closure

- An incident shall be closed only after:
  - Issue is fully resolved
  - Business impact is addressed
  - Management approval obtained for critical incidents

9. Incident Documentation & Record Keeping

- An **Incident Register / Log** shall be maintained by IT.
- Incident records shall be retained for audit and review purposes.

10. Third-Party Incidents

- Incidents involving third-party systems or access shall be coordinated with the concerned vendor.
- Access provided to third parties during incident resolution shall be time-bound and monitored.

11. Compliance & Disciplinary Action

Non-compliance with this policy may result in disciplinary action and may attract legal consequences.

12. Policy Review

This policy shall be reviewed periodically and updated as required.

FUJIYAMA POWER SYSTEMS LIMITED

Information Security Policy

1. Objective

To protect the Company's information assets from unauthorized access, disclosure, alteration, and destruction, and to ensure confidentiality, integrity, and availability of information.

2. Scope

This policy applies to:

- All employees, contractual staff, consultants, and third parties
- All information assets including data, systems, applications (including BUSY), servers, laptops, desktops, networks, and backups

3. Information Security Responsibilities

- **Management**: Overall responsibility for information security
- **IT Department**: Implementation and monitoring of security controls
- **Users**: Compliance with this policy and safeguarding credentials
- **Internal Auditor**: Periodic review of policy compliance

4. Access Control

- Access to systems and applications shall be provided strictly on a **need-to-know** basis.
- User IDs and passwords shall not be shared.
- Access provisioning, modification, and revocation shall follow the **Access Management Procedure**.
- User access shall be reviewed periodically.

5. Password & Authentication Security

- Strong passwords shall be used for all systems.
- Passwords shall be kept confidential and changed periodically.
- Default and shared passwords shall be avoided wherever possible.

6. Data Protection & Confidentiality

- Confidential and sensitive data shall be protected from unauthorized access.
- Data shall be used only for official business purposes.
- Backup of critical data shall be taken periodically and stored securely.

7. System & Network Security

- Antivirus and security updates shall be installed on systems where applicable.
- Unauthorized software installation is prohibited.

- Remote access shall be permitted only with management approval and adequate security controls.

8. Incident Management

- Any actual or suspected information security incident (data breach, malware, unauthorized access, data loss) shall be reported immediately to the IT Department.
- Incidents shall be investigated and corrective actions shall be taken.

9. Third-Party Security

- Third-party access to systems shall be approved, limited, and time-bound.
- Third parties shall comply with Company information security requirements.

10. Compliance & Disciplinary Action

Violation of this policy may result in disciplinary action and may also attract legal consequences.

11. Policy Review

This policy shall be reviewed periodically and updated as required.

FUJIYAMA POWER SYSTEMS LIMITED

Password Policy

1. Purpose

This policy defines basic requirements for creation, use, and management of passwords to protect Company systems and information.

2. Scope

Applicable to all employees and users who access Company systems.

3. Password Allocation and Use

- New user IDs are created and allotted by the **IT Department**.
- Initial passwords are set by the **IT Department** and shared securely with the user.
- Users are provided an **option to change the password**, which they may change later as required.
- Passwords must be kept confidential and must not be shared with anyone.

4. Password Change and Validity

- Passwords should be changed periodically, where technically feasible.
- When IT resets or issues a password, it is treated as a **temporary password**, and users are encouraged to change it at first login.

5. User Exit and Access Deactivation

- When a user leaves the Company or access is no longer required, the **IT Department shall deactivate the user ID and system access** based on information received from HR or Management.

6. Enforcement

Non-compliance with this policy may lead to restriction or withdrawal of system access, as per Management decision.

FUJIYAMA POWER SYSTEMS LIMITED

Physical Security Policy

1. Objective

To protect Company premises, information assets, IT infrastructure, and personnel from unauthorized physical access, damage, theft, or disruption.

2. Scope

This policy applies to:

- All Company offices, plants, warehouses, and premises
- IT infrastructure including servers, desktops, laptops, networking equipment, and storage devices
- All employees, contract staff, visitors, and third parties

3. Roles & Responsibilities

- **Management**: Overall responsibility for physical security
- **Administration / Security Team**: Implementation and monitoring of physical security controls
- **IT Department**: Physical security of IT equipment and data storage devices
- **Employees**: Compliance with physical security requirements
- **Internal Auditor**: Periodic review of compliance

4. Access to Premises

- Entry to Company premises shall be restricted to authorized personnel only.
- Visitors shall be allowed entry only with prior authorization and shall be escorted where required.
- Visitor entry and exit shall be recorded by the security guard.

5. Physical Access Controls

- Office areas, server rooms, and locations housing critical IT equipment shall be secured.
- Access to server rooms and critical IT infrastructure shall be limited to authorized personnel.
- Keys, access cards, or biometric access (where applicable) shall be controlled and monitored.

6. Security of IT Assets

- IT equipment shall be protected against theft, damage, and unauthorized access.
- Laptops and portable devices shall be secured when not in use.
- Removal of IT assets from Company premises shall require prior authorization.

7. Environmental & Safety Controls

- Fire safety measures such as fire extinguishers shall be available as per applicable regulations.
- Critical IT equipment shall be protected from environmental risks such as water leakage, excessive heat, or dust.

8. Third-Party & Vendor Access

- Third-party access to Company premises shall be authorized, monitored, and limited to business requirements.
- Access to sensitive areas shall be supervised.

9. Incident Reporting

- Any physical security incident (theft, unauthorized entry, damage to assets) shall be reported immediately to management and the Administration / IT Department.
- Incidents shall be investigated and documented as per the Incident Management Policy.

10. Compliance & Disciplinary Action

Violation of this policy may result in disciplinary action and may also attract legal consequences.

11. Policy Review

This policy shall be reviewed periodically and updated as required.