Use of IT Resource Policy

1. INTRODUCTION

1.1. Purpose

SYBRID provides its employees with access to Information Technology (IT) resources as required for the performance and fulfillment of job duties. This policy defines the responsibilities of both the SYBRID and the employee in regard to these resources.

1.2. Scope of Applicability

This policy applies to all employees, personnel from other organizations, contracting personnel, and vendors using IT Resources and Systems of SYBRID.

2. POLICY

2.1. Overview of Technologies

1. SYBRID defines two types of IT resources; technologies that create records, and those that do not.
    a. Those that create records include, but may not be limited to, computer software, the Internet, the Intranet, e-mail, fax, voice mail, and any emerging technologies.
    b. Those that do not create records include, but may not be limited to, computer hardware, telephones, cell phones, pagers, and other communication devices.

2.2. SYBRID Responsibilities

1. SYBRID has the right to monitor and review employee use as required for legal, audit, or legitimate authorized operational or management purposes.

2.3. Employee Responsibilities

1. Only minimal personal use of SYBRID IT resources is allowed, and should not interfere with the legitimate business of SYBRID.
2. Access to any SYBRID IT resource may be denied or revoked at any time for any reason without notice.
3. Users of workstations (desktop machines / laptops) are restricted to install any software and software installation can only be done through Administrative account which is owned by IT department.
4. Access and privileges on SYBRID applications systems are assigned and managed by the administrators of specific systems. Eligible individuals may become authorized users of a resource or system and be granted appropriate access and privileges by following the approval steps for that resource or system.
5. Inappropriate use of SYBRID IT resources posing the risk of disruption to business activities is prohibited. (See Appendix B)
6. Employees will be informed about confidentiality, privacy, and acceptable use of SYBRID IT resources as defined in this policy. Detailed information is available in the following appendices:
    a. Appendix A - Responsibilities
    b. Appendix B - Unacceptable Use of IT Resources

2.4. Acceptable Email Use

1. SYBRID e-mail system consists of a network of servers and network devices administered and maintained by IT Manager. Within this e-mail system, all messages, attachments, files, and folders are automatically scanned for viruses.
2. All Departments and/or Offices within SYBRID are responsible for the e-mail activities of their employees.
3. All messages sent or received using these e-mail resources are owned by the SYBRID and may be considered Departmental records.
4. The SYBRID reserves the right to monitor and/or log all e-mail communications without notice. Employees should have no expectation of privacy in the use of the e-mail system.

2.4.1. Employee Responsibility

1. Employees must use the SYBRID e-mail system for all e-mail correspondence.
2. Only minimal personal use of the SYBRID e-mail system is allowed, and should not interfere with the legitimate business.
3. All e-mail correspondence is considered the property of the SYBRID.
4. Employees must follow specific guidelines when sending mass mailings or group messages.
5. Employees must be aware of rules regarding e-mail attachments.
6. Employees must use secure passwords.

2.4.2. Employee E-mail Retention Requirements

1. E-mail messages sent or received in the course of business transactions are SYBRID records and must be retained by the employee - in either hard copy or electronic format - for as long as they are needed to meet SYBRID requirements.
2. Informational e-mail messages are non-records. These messages are generally of temporary value and do not need to be collected and maintained into a record keeping system.

2.4.3. E-mail Systems Administrators Retention Requirements

1. E-mail system administrators will retain general back-up files for disaster recovery purposes only.
2. Copies of e-mail messages held on back-up systems will remain accessible and may be subject to discovery and monitoring processes.
3. E-mail messages older than [90] days may be purged from the system.

2.4.4. Authorized Access to E-mail Messages

1. The IT Manager will not routinely monitor e-mail but may, with prior authorization, access and/or disclose the e-mail or files of an employee with just cause, provided it follows appropriate procedures designed to assure compliance with SYBRID policies. Just cause may include the following:
    a. To protect system security;
    b. To fulfill SYBRID obligations;

c. To detect employee wrongdoing;

d. To comply with legal procedures;

e. To protect the rights or property of the SYBRID.

2. Any supervisor or manager may request access to the e-mail messages of their employees.
3. If it becomes necessary to access an employee's e-mail to complete urgent SYBRID business, supervisors or managers may request immediate access by contacting the IT Manager.
4. The IT Manager will maintain a file of supporting documentation of all authorized access to e-mail messages.

2.4.5. Conditions of Disclosure of E-mail Information

1. The contents of e-mail messages properly obtained for Departmental purposes may be disclosed within the SYBRID for an official purpose without the permission of the authorized user who created the message.
2. SYBRID will attempt to refrain from disclosure of particular communications if it appears likely to create personal embarrassment, unless such disclosure is required to serve a Departmental purpose or to satisfy a legal obligation.

2.5. Acceptable Computer Use

1. Computer workstations installed for use within the SYBRID are the property of the SYBRID, and are provided to assist SYBRID employees in performing their duties and responsibilities associated with their positions and in support of business functions.
2. SYBRID employees and authorized network users can log on to the network from any computer in the SYBRID network to gain access to their e-mail, personal and shared network areas, as well as most other applications to which they are authorized to access.
3. Only minimal personal use of SYBRID computing devices is allowed, and should not interfere with the legitimate business of the Organization.
4. Transactions resulting from computer usage are the property of the SYBRID, and are subject to SYBRID policies as well as all applicable statutory laws.
5. Departments/Offices may revoke the access rights of any individual at any time in order to protect data or to preserve the functionality of electronic information systems.
6. IT Manager in consent with ISM will evaluate, authorize, install, and maintain all software and hardware for use on all SYBRID desktop computers, laptops, servers, and other computing devices.

2.5.1. Employee Responsibilities

1. Users of the SYBRID workstations and authorized network users are responsible for becoming familiar with and abiding by all SYBRID IT policies and procedures.
2. Each network user is responsible for logging out of applications and the network when vacating a shared computer, and for locking or logging off their workstation when not in use.
3. Network users are not permitted to share their userid or password(s), or leave workstations unlocked or unattended.

4. SYBRID network users are prohibited from downloading, attaching, installing, or changing any software or hardware, including wireless devices.
5. Vendors, visitors and/or non-SYBRID employees are prohibited from connecting equipment (including laptops) to the SYBRID network without specific authorization by IT Manager.

2.5.2. Unauthorized Uses of SYBRID Workstations

1. All activities performed on workstations can affect the availability of resources for part of, or the entire SYBRID network. Unauthorized uses of SYBRID workstations include, but may not be limited to the following:
    a. Bypassing or attempting to bypass security and access control systems;
    b. Using workstations to play or download games, or broadcast audio or video for non-business functions;
    c. Access non-SYBRID provided web e-mail services;
    d. Unauthorized use of Instant Messaging or Internet Relay Chat (IRC);
    e. Utilizing unauthorized peer-to-peer networking or peer-to-peer file sharing;
    f. Sending or sharing confidential information for unauthorized purposes; or
    g. Using the workstation for activities other than its intended purpose including those that violate any local law or any other statutory or SYBRID policy.

2.6. Privacy Issues and Legal Implications

1. Employees should have no expectation of privacy while using SYBRID IT Resources.
2. E-mail and other electronic files create a record and may be accessible through the discovery process in the event of litigation.

2.7. Retention/Disposition of IT Records

1. IT records are retained or disposed of in accordance with the policies and regulations associated with those records.

2.8. Enforcement Authority

1. The IT Manager has been designated by the CEO to monitor and provide initial enforcement of SYBRID's IT policies.
2. The Information Security Manager is the authority who investigates reported instances of Departmental employee misconduct.

2.9. Violations and Disciplinary Action(s)

1. All suspected violations of this policy will be reported to a supervisor in the chain of command above the employee.
2. The supervisor or designee will review the facts; and if it is suspected that a violation may have occurred, the matter will be referred to the Information Security Manager for appropriate action.
3. As determined by the Information Security Manager, instances of abuse or misconduct, depending on the circumstances, will be referred to Administration Department / HR DEPARTMENT for further investigation.

4. Employees who willfully or knowingly violate or otherwise abuse the provisions of this policy may be subject to disciplinary action as outlined in [SYBRID DAC].

Appendix A – Employee Responsibilities

Employees should conduct themselves as representatives of SYBRID Private Limited.

1. Employees will only access files, data, and protected records if:
   a. the employee owns the information;
   b. the employee is authorized to receive the information; or
   c. the information is publicly available.
2. Employees are responsible for all activity that comes from their computer. For example, employees must:
   a. always use strong passwords; and
   b. NEVER share passwords with any individual for any reason
3. Employees must guard against access to files and take precautions to protect IT devices when away from the workstation. This will include but may not be limited to the following:
   a. logging off computer;
   b. locking computer; and/or
   c. locking file drawers
4. Employees are prohibited from monopolizing systems; overloading networks with excessive data; or wasting computer time, connect time, bandwidth, disk space, printer paper, or other IT resources.
5. Employees are prohibited from transmitting personal information about themselves or someone else using SYBRID-provided IT resources without proper authorization.
6. Employees must report the following instances to a supervisor or appropriate authority:
   a. receiving or obtaining information to which the employee is not entitled (Note: the owner or sender of such information must also be notified);
   b. becoming aware of breaches in security; or
   c. becoming aware of any inappropriate use of SYBRID-provided IT resource.
7. Employees will contact an immediate supervisor if there is doubt concerning authorization to access any SYBRID-provided IT resource.
8. Employees must adhere to copyright law regarding the use of software, print or electric information, and attributions of authorship.

Appendix B – Unacceptable Uses of IT Resources

1. Employees will not use SYBRID-provided IT resources for inappropriate purposes or in support of such activities. This includes, but is not limited to the following:
    a. any use which violates statutory regulations, or any applicable laws;
    b. any use for commercial purposes, product advertisements, or “for-profit” personal activity;
    c. any use for viewing, transmitting, receiving, saving, or printing sexually explicit material;
    d. any use for religious or political lobbying;
    e. any use in relation to copyright infringement;
    f. any use of the Internet other than for official business;
    g. any use in relation to downloading or installing any software or inappropriate files (ex:MP3 files);
    h. any use in relation to participating in chain letters or chat programs;
    i. any use for promoting discrimination on the basis of race, gender, national origin, age, marital status, sexual orientation, religion, or disability;
    j. any use for promoting the use of weapons or devices associated with terrorist activities;
    k. any use for dispersing data to customers or clients without authorization; or
    l. any use in relation to gambling
2. Employees will not waste IT resources by intentionally doing one or more of the following:
    a. placing a program in an endless loop;
    b. printing unnecessary amounts of paper;
    c. disrupting the use or performance of SYBRID-provided IT resources or any other computer system or network; or
    d. storing unauthorized information or software on SYBRID-provided IT resources.
3. Employees will not knowingly or inadvertently commit security violations. This includes doing one or more of the following:
    a. accessing records within or outside the SYBRID’s computer and communications facilities for which the employee is not authorized;
    b. copying, disclosing, transferring, examining, re-naming, or changing information or programs belonging to another user unless given express permission to do so by the user responsible for the information or programs; or
    c. violating the privacy of individual users by reading e-mail or private communications unless the employee is specifically authorized to maintain and support the system.
4. Employees will not knowingly or inadvertently spread computer viruses. To reduce this threat, employees must not import files from unknown or questionable sources.