Applied BioCode, Inc.

Information Technology Governance and Control

Version	Date
5	2022.04

Contents

Title	**Process Owner**
Administrative and Marketing Director	April Tang
Senior IT Specialist	Cliff Chang
IT Manager	Dennis Chou
Jr. IT Engineer	Laurence Tung

System	**Module**
Windows Server Backup	Datto Siris 4 Professional

Report Name	**System**
User Access Request Form	
Asset Decommission Form	
Employee Termination Form	
Employee Asset Assignment Form	

Functions and Responsibilities of IT Department

The primary function of IT Department is to maintain the company-wide management information system and ensure the sufficient security control has been established for information flow.

Duties of IT Department

- Establish and maintain computerized information policy
- Conduct system or program development, maintenance of computer hardware and security management, including information network setup and maintenance.
- Manage users' password and access right setup.
- Problem solving of hardware / software malfunction issues throughout the company.
- Provide user training and operating procedures as required.

Responsibility of user [Employees, Consultants]

- Compile with the relevant procedure and policy related to computerized information.
- Request system improvement or enhancement based on general operating requirements and work-related demands.
- Authorization of system access and privileges must be granted by IT for specific departments or individuals according to responsibilities.
- Assist to evaluate the performance of system or program and services provide by the outsourcing vendors.

The company should establish IT Security Event Response Unit and give a clear definition to its members' job role, and the members have clear understanding of their roles. If an IT Security Event occurs, the IT Security Event Response Unit will be in charge, record the occurrence and response measures in IT Security Event Handling Report, send to approval by the Responsible Manager, and report to related department.

Documentation of system or program development process

All process of system development or change performed by IT Department or outsourcing vendors should be documented properly. Relevant documentation should include system feature, installation instructions, program change documents, system testing records, acknowledge of acceptance and user guides. All relevant documentations should be modified in accordance with changes made to the system or program.

User guides for outsourced or self-developed system or program should be provided to the users and kept in the user department. Other documents of system or program should be kept and managed by IT Department in a custody place. The documents of system or program should be coded in the sequential number and the list of documents of system or program should be maintained by the responsible personnel. For tracking purpose, a log should be maintained to record the number and name of documents, date of borrowing, reason, and signature of borrowers. The outdated system documents should be disposed with proper approval form authorized personnel.

Applications, Databases, and Operating Systems Access

Access to applications, databases, and operating systems is subject to authentication using passwords. The password of all user accounts authenticated in Applications, Databases, and Operating Systems are required to use the complex password (alphanumeric with special character) and should be changed every 90 days. The password is at least eight characters long. The same password cannot be reused for next four (4) changes. System will lock the user account if there are 3 failed login attempts.

All requests for new user access for Applications, Databases, and Operating Systems must be documented and approved by an appropriate level of management. If a user requires additional access, they must fill out the User Access Request form which will be approved by their supervisor and IT department.

When an employee is terminated, Management will inform the IT department to disable the account and update applications, databases and active directory access. The IT department will change the password or disable the account, so terminated employees cannot access the Applications, Databases and Operating Systems directory. The terminated employee account is entirely removed or locked from the systems.

Direct data modifications are documented and appropriately approved by the authorized management prior to changes being made in production.

Reviews of Applications, Databases, and Operating Systems access are on a periodic basis and are properly reviewed and approved by IT personnel.

Network Access

The Company uses proper tools to manage the network access. And considers the different IT services, users, applicational system characteristics, appropriately separate the web domains to protect important system and data.

The user is required to use a complex password (alphanumeric with special character) and change it every 90 days. The password frequency rule applies to the Company Accounting System. The password is at least eight characters long. Indeed, the same password cannot be reused for next four (4) changes.

When a new employee joins the Company, the authorized management informs the IT department. The Senior IT adds the new user to the network and provides access network to the directory and system based on email notification. IT will provide the user a temporary password which the user changes at the first login. If a user requires additional network directory access, the management requests the additional access with the User Access Request Form. The IT department will file the request in Access Request form before asking for updated access.

When an employee is terminated, management will inform the IT department to disable the account and update network directory access. The IT department will change the password, so that the terminated employee cannot access the network and directory before archiving the data.

If a user requires VPN access, they must receive approval from their supervisor and the IT department by filling out the User Access Request form.

Software Lifecycle

Most of the software is off the shelf product. The Company does not develop perpetual software. Consultants are used to design and implement the software with in-house user's oversight.

When the company has software and hardware maintenance requirement and inquire contracted development or maintenance service, is required to review, according to the nature of contracted service, the content shall include but not limited to contract schedule, completion date, maintenance procedure, payment procedure, property rights, software and hardware requirement, deployment documents, penalty compensation and necessary safety measures, to protect the company's rights.

Minor change less than $1,000 and does not modify the data table can be processed without a Change Request Form. The change equal to or greater than $1,000 or amend the data table requires a Change Request Form to proceed.

The consultant designs and reports the status to the process owner. The process owner assigns a user to perform alpha, beta, and user's acceptance testing (UAT) before finalizing the development. The UAT validates the data completeness and accuracy. The user documents the testing method for process owner approval before conducting the test and reporting the deliverable to the process owner. **The Process Owner reviews the resulted before accepting the product and scheduled the go-live date in the in System Changed Requested.**

Before go-live date, the company's IT staff should manage and control the software versions, backup previous versions and keep appropriate records, to ensure the system will not fail to resume previous versions shall the new software version proves to be inadequate. The sensitive application and database are designated to a restricted directory.

Back-Up and Restoration

The Company performs daily backup. Backup for important programs, related documents, and source data should be performed and stored at offsite location or online, if applicable. Based on the sensitivity of network directory, the backup file can be incremental or full. Following is the backup file requirement and rotation.

Frequency	**Retention Period**
Daily	Archive for 7 days
Weekly	Archive for 4 weeks
Quarterly	Archive indefinitely

When a user requires a file to be restored, the user requests the file with IT department will**. If the data stored is in a sensitive network directory, the requestor needs to obtain approval for IT department to restore from the backup.** The backup file is restored to a temporary directory for the user to review and transfer the file to the appropriate directory.

IT department will perform semi-annual restore testing via hap hazardously selecting a backup file from the prior month and restore to a temp directory. The file is opened to confirm the integrity of the restore file.

Information System Disaster Recovery

1. The company shall create Disaster Recovery Rehearsal plan, define the rehearsal's objectives and each responsible person's job role, and define Recovery Time Objective (RTO) according to the company's risk management.

2. The company shall perform the Disaster Recovery Rehearsal, the testing result recorded by the IT staff, and combined with the testing data to send to approval by the Responsible Manager and then keep storage.

Accounting Record

The input and output control for the accounting record is discussed in the *Period End and Financial Document.*

Acquisition and Disposal

The IT executed the Company Capital Assets policy for acquisition and disposal, *see Acquisition to Disposal Document.*

The IT shall back up all system data or files saved in the hard desk drive before disposal of the IT asset and save the backup data to the new computer or other backup devices.

The IT shall complete the entire secure information disposal procedures, including reformate hard disk drive, remove the operating system, data, and system application with registered copyright, and physically destroy (for example, shred or wreck) the disk or CD.

Safeguarding

The Company has a periodic checklist to ensure the hardware and software is in a working condition and limiting the downtime. The checklist is documented and archived by Senior QA Specialist.

The Company installs the anti-virus software to scan network and desktop files. The desktop user cannot edit the anti-virus scan and update scheduled.

The Company Property and Technology Usage are disclosed in the employee handbook. New employee acknowledges the receipt of handbook and understanding of policy. Amended policy is informed to all employees via email and ADP Time and Attendance screen.

After 3 unsuccessful network logins within 30 minutes, the system locks the user account. User contacts the IT department to assign a temporary password for network access. The IT department will investigate the root caused for example user fails login or unauthorized access attempts. If necessary, the unauthorized access attempt is documented and reported to authorized management

The hardware is locked in a secure room. The unauthorized visitors are logged and escorted by the authorized staff. The IT department will test the UPC power and clean the airway of hardware quarterly.

The Company does not have ecommerce or significant external traffic risk to perform the network vulnerability testing.

Information flow security inspection

Important software and data files should be encrypted, and passwords should be updated on a regular basis.

Information security should be reviewed by IT Department annually to avoid unauthorized software, duplication and illegal breach of data.

Information disclosed on the Company's websites should be reviewed by responsible personnel periodically and removed sensitive and confidential information immediately.

The control procedures incorporated in the computerized information process should be included in the annual audit plan and conducted by the internal auditor based on the control frequency.

Employees shall avoid submitting, receiving, or downloading e-mail or software unrelated to the job function via the company's internet, to prevent company's internet resource occupation, and computer attack vulnerabilities.

Disclosing and reporting information on websites designated by the FSC

The equipment, system, internet connection should be set up and maintained by IT Department for posting information required by FSC in the reporting system.

Online reporting system access, user account and password should be assessed by management with due care and only granted to reliable personnel for accessing and uploading company information. The password should be changed with sufficient complexity at first login and periodically.

The additional access, user account and password should be kept by the authorized personnel in a custody place.

Company should declare public information and significant matters in accordance with relevant laws and regulations and disclosing information within the required time frame.

All uploading files should be reviewed and approved by responsible supervisor to ensure the completeness and accuracy of the content.