Standard Policy & Procedure

SPP 604

Information Security Policy

Version: 1.0 (draft)

Revision History

Date	Version	Revision Description	Author
04/01/2021	1.1	Reviewed; updated for company Name change	Ram Pal Sharma

Document Approval

These functions (or their designees) have responsibility for approving, drafting, revising, and enforcing this policy.

Name	Title
Nitin Sharma	Head IT
Ram Pal Sharma	Asst. Manager IT

Questions

In the event of questions or comments about this policy, please contact Beetel IT Team.

Table of Contents

1. Purpose

The purpose of this policy is to protect the systems infrastructure and information assets of Beetel and its subsidiaries and affiliates (collectively referred to as the “company”) by establishing the proper use and protection of Beetel’s IT resources and information.

2. Scope

This policy is applicable to all employees, consultants, contract personnel, vendors, contractors, and personnel providing services to Beetel (collectively “Beetel Personnel”), including its wholly-owned subsidiaries, their wholly-owned subsidiaries, and affiliated companies (by way of example: a majority owned Joint Venture (JV)), operating units and divisions, domestic and foreign (“Beetel”).

This policy also applies to all IT assets and systems owned or operated by “Beetel Personnel”.

3. Definitions

For the purposes of this policy, the following terms shall have the following meanings:

- **Information Security.** This policy defines information security as the protection of information from loss of confidentiality, integrity and/or availability.

- **CHD.** Cardholder Data. Includes the full primary account number and other information regarding credit cards including cardholder name, expiration date, and service code.

- **Control**. The policies plans and procedures, and organizational structures designed to provide reasonable assurance that business objectives will be achieved, and undesired events will be prevented or detected and corrected.

- **Control Framework**. A set of fundamental controls that facilitates the discharge of business process owner responsibilities to prevent financial or information loss in an organization.

- **Control Objective**. A statement of the desired result or purpose to be achieved by implementing control procedures in a process.

- **DMZ.** A DMZ or demilitarized zone (sometimes referred to as a perimeter network) is a physical or logical subnetwork that contains and exposes an organization’s external-facing services to an untrusted network, usually a larger network such as the internet.

- **Risk**. The potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss and/or damage to the assets; usually measured by a combination of impact and probability of occurrence.

- **Segregation of Duties**. A basic internal control that prevents or detects errors and irregularities by assigning responsibility for initiating and recording transactions and custody of assets to separate individuals. Commonly used in large IT organizations so that no single person can introduce fraudulent or malicious code without detection.

- **Sensitive Authentication Data.** Security related information including, but not limited to, credit card validation codes/Values, full magnetic stripe data, PINs used to authenticate cardholders and or authorize payment card transactions.

- **System.** Refers to the entire computer network, including, without limitation, servers, desktops, laptops, tablets, handheld computers, PDAs, cell phones, smartphones, telephones, voicemail, software, telecommunications equipment, peripheral devices, the internal/external computer and communications network and any data/information contained or processed by such network, email system, Intranet, company web sites, and access to the Internet.

- **PAN.** Primary Account Number refers to payment card number (credit or debit) that identifies the issuer and the cardholder account

- **Vulnerability Management.** The "cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities", especially in software and firmware.

4. Information Security Objectives

Information is an essential asset. It is crucial that information is available, correct and confidential. This policy seeks to assist Beetel in achieving the following information security objectives:

Objective	What does it mean?	Examples
Confidentiality	Ensure that information will not be disclosed to anyone who is not authorized to access it. The confidentiality of information, including during processing, should be safeguarded by appropriate measures in respect to protection and classification.	• protection of authentication data • protection of confidential or secret data • protection of personal data
Integrity	Ensure that information is accurate and complete. The quality of information processing should be maintained. It should be possible to verify the integrity of data at points during the processing phase.	• Protection from the manipulation of orders, pricing data etc. • Protection from the manipulation of services (e. g. through viruses, Trojan horses).
Availability	Ensure that information is available when required. The availability of IT, as well as the functioning of specific services, should be guaranteed to meet the requirements of the business.	• reliability during the service provision • access to data on schedule
Non-repudiation	Protect the authorship of data and ensure that there is no question of the source	• undeniable proof of user transactions, • to make more difficult the denial of contracts and financial transactions

Auditability	Ensure IT-related processing is traceable by means of logging relevant information. The audit trail allows checking the validity of information sources and changes made to that information. Events putting the security of IT systems in unacceptable level of danger should trigger immediate action.	• security event logging (e.g. log on) • user activity logging (e.g. data entry)

5. Policy

Beetel will protect information in such a way, that:

- privacy is protected in accordance with policies of Beetel
- the integrity of information is maintained
- information is available as required and necessary
- transactions cannot be repudiated
- legal and contractual obligations can be fulfilled
- information owners are identified and appointed for information considered to be of a commercially sensitive or of confidential nature
- all users and staff act responsibly in handling commercially sensitive or confidential information
- it is possible to audit transactions and events that are critical to ensuring information security
- preventive measures should have priority over reactive damage control
- where possible, security measures must be supported or enforced by technical solutions

6. Security Awareness

IT security is an increasingly important factor to the daily business that Beetel undertakes. Accordingly, an awareness of IT security is a crucial factor for Beetel.

IT security awareness is characterized by:

- seeing clearly that security is a critical and substantial item of Beetel’s business philosophy
  • security awareness existing within all daily activities, whether by the business or IT
- personal responsibility by Beetel staff to take the appropriate measures to identify and minimize risks that threaten Beetel’s IT resources and data.

Beetel will seek to build this information security awareness by:

- ensuring information security is considered an important topic by Beetel management
- delivering appropriate communications around IT security
- providing up to date information to staff about security issues of relevance to Beetel.
- Ensuring that all the information security policies are reviewed and updated on an annual basis.

7. Access Security

7.1 Application Access Security

Formal guidelines for access to applications should be established to ensure appropriate access is added, changed, and removed. This includes applications managed internally by Beetel Teletech Ltd.. or externally by a third party. This applies to all Beetel Personnel and to all other individuals who directly or indirectly use or support the services or information of Beetel.

7.2 User Access Management

Please refer to SPP610 User Access Management Policy.

7.3 Usernames

A unique identification (ID) will be assigned to each person with access to systems to ensure that everyone is uniquely accountable for their actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users and processes.

7.4 Application Logon

Access to business systems and applications must occur through a secure logon process. The procedure for logging into a computer system (e.g. login) must be designed to minimize the risk of unauthorized access.

The identity of the user must be authenticated before giving access to the application or system with a procedure that is adapted to the sensitivity of the protected application, system or information in question.

It is recognized that the strength of security around logon is restricted to the technology of the production system or application in question, especially for legacy systems. As such where it is not possible to implement such controls this guideline must be considered when designing or procuring a new IT solution that will be storing highly sensitive or confidential data.

Each Beetel organization should maintain a current list of applications which, due to technology reasons, cannot meet the password and logon requirements, and document any mitigating controls or roadmaps for replacement.

7.5 Logging and Reporting of System Access

Where technically possible, applications and systems must log and thus permit monitoring of key system access and usage events. Examples of key system access and usage events include:

- Successful and unsuccessful logons and logoffs.
- Unauthorized access attempts.
- Access failures to sensitive or commercial information as required by the designated information owner.
- Account access changes
- Account additions and removals
- Changes of security related parameters and tables, especially access profiles and permissions.

Security logs should be kept for at least a year or more depending on the sensitivity/data type to assist in future investigations and access control monitoring. (Ref SPP 707 Records Retention)

Where possible appropriate reporting, monitoring or alerting tools should be used to improve the efficiency of these reviews.

It is recognized the strength of security around security event monitoring is restricted by the technology and inherent design of the production system or application in question. This is particularly pertinent for legacy systems and off-the-shelf systems where Beetel cannot enforce the desired level of security. In those cases, the technical limitations should be documented, and compensating controls should be used to assist in the monitoring of systems access.

7.6 Audit Log Reviews

Where Applicable and available, audit logs should be reviewed to help identifying anomalies or suspicious activity using the following methods:

- ✦ All security events
- ✦ Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD
- ✦ Logs of all critical system components
- ✦ Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems, authentication servers, e-commerce redirection servers, etc.)
- ✦ Any anomalies or exceptions discovered by log review must be followed up on.

7.7 Direct Data Access

Direct data access to applications must be restricted to authorized resources. Direct data access is defined as the ability to modify access and modify data at the data storage layer. Allowing direct data access diminishes the confidentiality, integrity, non-repudiation, and auditability quality of data and should be considered a means of last resort. Accounts with the ability to directly access and modify data must be reviewed on a regular basis.

8 Password Policy

Please refer to SPP606 – Password policy

9 E-mail Security

Improper e-mail usage binds resources (e. g. disk space, bandwidth, and productivity) and may expose Beetel to availability issues.

Messages should be addressed to recipients on a need-to-know basis. Messages sent unnecessarily can impact system and user performance.

E-mail to all staff (enterprise-wide) is reserved for very important messages and needs the approval of appropriate Beetel management.

It is prohibited for any user to originate or distribute any chain letters by e-mail.

It is prohibited to transmit unencrypted Primary Account Numbers (PANs) over end-user messaging (including, but not limited to email, instant messaging, or chat).

For additional guidance on email usage please refer to SPP 602 - Email Usage Standard.

9.1 User Termination

a. Requests to access data from a terminated user’s laptop or email must receive approval from reporting manger or Human resource.

b. Once Human Resource submits a termination notice, IT reserves the right to make a backup of the data and save to a restricted share drive. After 90 days, backups should be deleted, unless required.

9.2 E-mail Attachments

File attachments are the most common method for transmitting viruses via e-mail. Care must be taken to ensure that file attachments are from a viable and trusted source. Their content should be known before opening or sending.

All email – with or without attachments – must be scanned, filtered and quarantined as required. If an attachment is found to be infected with a virus or not meet standards that allow its delivery, it may be quarantined at which point the user will not receive the email or receive the email but without the attachment.

If the attachment is needed and does not carry a threat to Beetel's security, IT can release it to the user, otherwise it will be discarded after an appropriate period.

Beetel will by default block attachments of non-common extensions, and others including .exe (executables), .bat (batch files), etc. that have been identified as potential threats.

9.3 Virus Checking

Each incoming e-mail must be checked for viruses and malware. This check should take place on the central mail gateway/server.

9.4 Confidentiality

Each e-mail should be managed according to the following:

9.4.1 Transport of e-mail thru Public Networks

Users must be careful when sending commercially sensitive or confidential information via email, especially to recipients outside the Beetel network. Users should limit the recipients of such emails to only those with a valid need to receive the information. Where possible confidential information should be sent via a secure method other than email (e.g. secure FTP connections). Please refer to SPP 603 and SPP 616 for more information.

9.4.2 Internal e-mail

E-mail messages, which are classified as internal, do not have to be secured unless, it is classified as commercially sensitive or confidential, and mechanisms for securing that information should be employed to protect the data.

9.5 Monitoring, Logging and Interception

Incoming and outgoing messages may be monitored as part of systems performance monitoring, maintenance, investigative, auditing or security activities. This is necessary to ensure the employee's proper use of e-mail and his or her compliance with internal policies or regulatory requirements.

If logging and monitoring tools are deployed, local Beetel operations must create strict guidelines on who can examine employee e-mail, and under what circumstances.

10 Systems Operations Security

Systems operations security contains guidance that must be followed for the operation of IT systems and resources within Beetel. The measures address the IT personnel which are responsible for the technical operation. It provides a minimum-security standard that should be followed for systems, operating systems and applications that are run by The Company.

A secure operation of Beetel's IT systems and infrastructure requires several safeguards and measures to be taken.

10.1 Personnel

IT security cannot be guaranteed by technical means only; therefore, the selection, training and organization of Beetel personnel are a vital factor that should be considered. IT personnel must be carefully selected with respect to the sensitivity of the IT systems under their control. Responsibilities for administration and maintenance tasks must be clearly defined and documented in writing. These roles should be segregated and separate from those that do development activities.

IT personnel should be trained for the administration and maintenance of the IT systems under their care as well as for general IT security issues and awareness.

Administrators must not use their privileges to read or access any information that is not needed for their work, unless this is part of a monitoring activity that was set up by IT Management or specifically and formally approved by senior management or Human Resources.

10.2 Security Incident Handling and Reporting

Please refer to SPP614 – Security Incident Management Procedure for further details.

All security incidents affecting customer systems or customer information must be reported to that customer's designated Information Security contact. It is the responsibility of the team handling the Security Incident (in accordance with SPP 614 Security Incident Management Procedure) to inform the customer in a timely manner.

10.3 Security patching

Patching of systems in a timely manner is a vital component of maintaining system security. Security patches should, in general, be applied within 30 days of release of patches, but no longer than 90 days. During official production change freeze periods, only critical emergency patching will be required. For further information, please refer to the SPP611 - Patch Management document.

10.3.1 Windows Security Patch Updates

Microsoft releases security patches the 2nd Tuesday of every month. Beetel, on or the day after, will perform an initial review of the patches. Preferably within 30 days, but for sure within 90 days, a Change Request Document (CRD) should be created and the patches implemented. This process will follow the IT Change Management policy.

Communications should be sent out to a global patching distribution group with the patches to be applied, the CRD numbers created, and the dates of implementation.

10.3.2 Linux Server and Other Device Patching

Linux servers should follow the same 180-day patching cycle. Other devices, such as network equipment, must be patched 180 days after any critical vulnerability is identified. These could be identified either by the quarterly network scan or any vendor communication.

10.3.3 Patch Vulnerability Management

Vulnerability management is integral to Beetel's computer and network security.

Of primary concern are vulnerabilities identified and given a critical severity, which must be remediated within 45. Vulnerabilities of high severity must be addressed within 60 days.

For further details, please refer to SPP613 - IT Vulnerability Management Policy.

11 Network Security

Please refer to the SPP605 - Network Security Policy.

12 Virus and Malware Protection

Windows production servers that support financially significant applications or data must be protected by antivirus software with current virus definitions. Prior to introducing new Windows based servers into Production, an antivirus client application with up-to-date virus definitions must be installed. All antivirus software must be kept current, actively run, can generate audit logs and be able to perform Microsoft system level file protection.

13 File Integrity Monitoring

For Servers in the DMZ or servers that store sensitive data, store/process/transmit credit card data, a change-detection mechanism such as file integrity monitoring tool must be deployed to alert Beetel Personnel of unauthorized modification of critical system files, configuration files or context files. These unauthorized changes could indicate a system compromise and should be investigated.

14 Disk Encryption Standard

This following are the requirements and guidelines for the use of disk encryption technologies on Beetel endpoint computing devices to protect the confidentiality of data at rest.

- Only whole disk encryption solutions approved by the Beetel IT Security Team may be utilized to satisfy the requirements of this policy
- The entire disk, or all user-writable local disk volumes, shall be encrypted.

- The whole disk encryption solution will centrally manage whole disk encryption client software for all systems, including encryption format, key management, and logging.
- Beetel will centrally maintain copies of encryption keys and encryption audit logs.
- Beetel retains the right to decrypt data using the centrally maintained key as required.

15 Solution Development Security

Solution Development Security includes guidelines for the development and the maintenance of IT systems that must be considered by IT development teams regardless of if they are employees, contractors or outsourcers.

15.1 New System Implementation

A new system may not be put into use unless it has been assessed against Beetel's information security policy and deemed to be appropriately compliant, especially regarding the nature of the information it manages. Security assessment criteria is included in the Solution Design Document as part of SPP 617 – System Development Lifecycle Policy

15.2 Secure Coding – Best Practices

Applications should be developed based on secure coding guidelines. As industry-accepted secure coding practices change, Beetel's coding practices should likewise be updated to address new threats.

15.3 Software development Policy

Refer to SPP617 – System Development Lifecycle Policy.

16 Physical Security

The Company manages both commercially sensitive and confidential commercial and personal information as part of providing services to our customers, and in our own business processes. As well as controlling access to Beetel's systems and data via security at the data center, network, and application level, we must also be aware of the need to prevent inappropriate access to our systems and data through Company's offices. Accordingly, all Company's offices will enforce security in our places of business via access control methods such as use of security badges.

16.1 Badges

The following procedures apply to anyone requiring access to badge access to Beetel facilities.

16.1.1 Authorized Users

Requests for badge access should be submitted and approved by Human Resources (HR-Admin and IT) or the requestor's manager. These requests should be maintained to show evidence of approval. Badge requests cannot be submitted by the individual requesting access.

16.1.2 Provisioning Badges

HR-Admin or IT or the requestor's manager will submit the approved request to Facilities Management for a new access badge. Facilities Management will provision appropriate level of access for access to Company facilities.

16.1.3 Terminating Access

When an employee or contractor separates from the company, the access badge must be disabled in a timely manner. HR and the manager must follow the personnel termination process. Access badges must be returned, and badge must be disabled.

16.1.4 User Responsibilities

All personnel with an access badge have a responsibility to protect their badge and the access rights it grants.

- User must not lend their access badge to anyone.
- User must not allow unauthorized individuals into any secure areas.
- User must not leave access badge unattended.
- User must immediately notify their manager and Facilities Management if their access badge is lost, stolen, or damaged.

16.2 Data Center Access

Access to the Data Center (or equipment room) housing servers must be restricted to individuals with an administrative need based on their job function.

17 Exceptions

Any exception to any part of the policy must be documented, reviewed, and approved by IT Senior Management. Exceptions should be evaluated annually or as necessary.

18 Miscellaneous

Compliance with Applicable Laws. In their use of the system, users must comply with all state, and Central laws, including those governing intellectual property and online activities. The company reserves the right to advise appropriate legal authorities of any potential violation of law by any user.

No Additional Rights. This Policy is not intended to and does not grant users any contractual rights.

19 Violation of policy

Violation of this policy can result in cancellation of system privileges and may result in disciplinary action, up to and including termination of employment, and/or potential legal action against the offending user. The Information Security Manager, or the appropriate designee must be notified immediately of any violations of this policy.

20 Local Laws and Regulations

The standards set out in this Policy are minimum requirements based on laws and regulations that generally apply to Beetel. Wherever local laws or regulations have requirements that differ, conflict with or are not included in this Policy, the relevant, local Beetel entity must consult with its local legal department or the Ethics & Compliance Office to determine which laws should apply.

21 Superseding Policy

Over the course of time other policies may have been written and adopted by Beetel Teletech Ltd.. or one of its subsidiaries that relate to or overlap with the subject matter in this policy. This policy supersedes all other formal or informal policies or documents containing policies dealing with the subject matter in this policy.

22 Aids

Beetel IT General Controls

24 Distribution

Beetel Teletech
Internal Use