**Personnel Security Policy And Procedure**

Doc ID:/POL/0.1

Document Classification: Internal

July 2022

**Document Control**

| Document Name | Personnel Security Policy and Procedure |
| --- | --- |
| Document ID | POL/0.1 |
| Security Classification | Internal |

| **Authorization** | | |
| --- | --- | --- |
| Document Owner | Reviewed by | Authorized by |
|  |  |  |

| **Amendment Log** | | | |
| --- | --- | --- | --- |
| **Version** | **Modification Date**  **DD MMM YYYY** | **Section** | **Brief description of the change** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**TABLE OF CONTENTS**

1.0 Purpose 4

2.0 Scope 4

3.0 Policy 4

3.1 Security in Job Definition 4

3.1.1 Recruitment Standards 4

3.2 Recruitment Process 5

3.2.1 Non-Disclosure Agreements 6

3.2.2 Terms and Conditions of employment 6

3.2.3 Including Information Security Norms in Job Responsibilities 6

3.2.4 Transfer and Termination Standards 6

3.2.5 Security Awareness and Training Sessions 6

3.2.6 Exit Procedure 7

3.3 User Responsibility/Accountability 7

3.3.1 Reporting Security Incidents and Weaknesses 7

3.3.2 Disciplinary Process 7

3.3.3 Handling of Information Security Breaches 8

4.0 Reference Documents 11

# Purpose

People are one of the most valuable information assets and it is necessary to address the risks of human error, theft, fraud or misuse of facilities and assist all employees in creating a secure computing environment.

# Scope

This policy applies to all employees, apprentices, contractors, consultants, temporary staff, third parties/vendors, etc. of Technovert. All are expected to be familiar with and comply with this policy.

# Policy

All the employees, apprentices, contractors, consultants, temporary staff, third party/vendor, trainees/interns, etc.

* Undergo personnel screening before joining
* Sign a confidentiality agreement
* Attend Information Security User Awareness Training
* Sign and Follow Acceptable Usage Policy and
* Be subject to disciplinary actions, for Information Security related misconduct

## Security in Job Definition

### Recruitment Standards

All applicants for the post of full-time employees or consultants shall be screened by the HR function as per the following process:

* Guidelines for HR administrators and/or hiring managers responsible for contacting employment references checks on prospective employees shall be done as mentioned below:
  + Post interview reference checks must be undertaken before recommending any candidate for appointment. This will normally be done via a structured phone interview with a minimum of at least two of the candidates’ nominated referees or another referee proposed by the nominated referee. Although this will mean that same-day offers will not always be possible, in the long run, this will maintain the integrity and quality of the candidates and recruitment process.
  + Any referee contacted must have worked closely, preferably in a senior position with the candidate and be in a position to comment knowledgeably about the candidate’s recent work performance. Applicants need to give prior permission to contact their referees and this should be obtained from the applicants. Existing employers of the prospective candidates would be contacted only on written consent by the candidates and in such situations the due diligence and checks would be more stringent and close probing would be mandatory.
  + Reference information sought must be job-related. Reference takers should cross-check and verify resume information and information provided by candidates during the interview with referees.
  + HR should protect the confidentiality of the process and the privacy of the applicant whenever possible by sharing only the information needed to secure the reference.
  + All reference check information should be recorded in writing in the form provided by Personnel. A separate form should be used for each reference check.
  + If negative information is obtained from a reference check, its accuracy should be verified from another source; it must be job-related. The alternative source should be from a similar rank/level as the first reference given, where possible. It may be necessary to request another referee from the candidate if the existing referees are not as senior as the source being verified. If still the information obtained is negative then the hire would not be considered suitable.
  + Any exceptions to the above reference check policy must be approved by the Management.
* For previous employment checks, educational backgrounds, physical fitness, address verification, and identity proof all employees or consultants shall submit the documents as mentioned in the joining formalities.
* If there is any change in the address the employee must submit a copy of the electricity bill/phone bill / Leave and License Agreement / Ownership Agreement Copy / Letter from the Housing Society for Permanent or Present Address for address verification.
* For criminal background, a copy of the Passport should be acceptable. In the absence of a Passport Copy, the candidate should produce a police clearance certificate within eight weeks of joining.
* Background checks shall be conducted if there is a need for the specific job profile or there is a client demand. *“Your employment with the company and continuance thereof is subject to your satisfactory reference and background checks. If, at any time, in the opinion of the Company, which shall be final, you become insolvent or are found to have provided incorrect or false information at the time of your selection or joining, guilty of dishonesty, disobedience, misappropriation, theft, fraud, disorderly behavior, negligence, indiscipline, absence from duty without permission or of any other conduct considered by the Company, as detrimental to its interests or violation of one or more terms of this appointment, your services may be terminated without notice. “*
* Immediate previous employment check before joining shall be done by taking the resignation acceptance letter or relieving letter of the previous organization. If required, the previous employer shall be contacted with the consent of the candidate.
* All contract staff, trainees, and temporary staff shall also be subjected to a similar screening process. A Non-Disclosure Agreement should be signed with the vendors/contractors. The contractual agreement with the contracted organization shall include a clause to assure that a similar screening process is being carried out for the contracted staff working for the organization. A standard employment agreement template shall be used. The contract staff/vendor employees when considered for permanent employment, the above screening process shall be repeated at the time of confirmation/appointment letter.
* All employees shall sign a Non-Disclosure Agreement (NDA) upon initiation of employment. The signed copy of the agreement shall be maintained along with other records of the employee with the HR.
* All the copies of documents collected should be verified with the originals at the time of joining.

## Recruitment Process

* + The HR should subject all selected candidates to screening, which includes background investigations as follows:
    - Availability of satisfactory reference checks.
    - A relevant background check with the help of third parties, need basis.
    - A check for completeness of the details of the applicant’s resume.
    - Confirmation of claimed academic and professional qualifications.
    - Independent identity check (Passport or similar document).
    - Relieving letter issued by the previous employer to be obtained from the candidate.
  + All employees should sign the following documents at the time of joining:
    - Agreements
    - Acceptance to Information Security Policy (Acceptable Usage Policy)
    - <<please update any other documents that are signed by the employee>>
  + The Internal Audit department should undertake a review of legal/regulatory requirements on a timely basis in consultation with the Legal representative and Management Representative to ensure continuous compliance.
  + All applicable issues should be analyzed and corrective actions, if any, should be promptly taken to ensure that the organization complies with the legal requirements.
  + Non-compliance with information security policies, standards, or procedures is grounds for disciplinary actions up to and including termination.

### Non-Disclosure Agreements

* NDA shall not be a part of the offer letter. NDA shall be part of the employment agreement / joining formalities for full-time employees, apprentices, and consultants at the time of joining. NDA shall be signed with the Vendor / Contractor for Vendor / Contractor employees. A standard employment agreement template shall be used.
* Employment agreement shall be signed by all full-time employees / direct contract employees/project trainees and deputed employees at the time of joining.
* The duly signed agreements will be maintained by the HR Team.

### Terms and Conditions of Employment

Terms and conditions of employment in the employment agreement should include the following:

* Legal and information security-related responsibilities like copyright laws or data protection legislations
* Signing and following of the Acceptable Usage Policy
* An indication of management action in case the terms of employment are violated
* The extent and duration of the responsibilities

The above terms and conditions shall also be included in the vendor/contractor’s SLA document.

### Including Information Security Norms in Job Responsibilities

* The terms and conditions of employment shall include employee responsibility towards complying with organizational Information Security as well as legal requirements.
* Security roles and responsibilities shall include any general responsibilities required for implementing or maintaining security policy, as well as any specific responsibilities for the protection of particular information assets or the execution of particular security processes or activities.

### Transfer and Termination Standards

* The HR shall send notification via e-mail but not limited to, about the transfer, resignation, suspension, or termination of services of any employee, to all concerned Department Heads / IT Team.
* The IT Team shall schedule the revocation of all logical access to information systems before providing a sign-off on the exit clearance form. The revocation process for logical access has been described in the Logical Access Control Policy and Procedure.
* The administration department shall ensure that the access keys (keys of the filing cabinets and storage shelves), and all equipment, are returned, before providing a signature on the clearance form.
* It is the responsibility of the respective project manager to ensure that all external consultants/contractors return access cards and other assets in their possession, if any, after completion of the assignment. It is the responsibility of the Project Manager to ensure that all the files, documents, manuals, brochures, and CDs / DVDs in possession of the employees, are returned before providing a signature on the clearance form.
* The HR department shall provide a final clearance only after all other required clearances have been obtained on the clearance form.

### Security Awareness and Training Sessions

* Users shall receive appropriate training on security requirements in the use/development of information systems, applications, and other information processing facilities.
* Users shall also be made aware of their security responsibilities and disciplinary process, which can be initiated against them in case of any violations of the organization’s policies and procedures.
* The HR department in co-ordination with the IT Team and Management Representative is responsible for designing and delivering security awareness sessions to existing employees regularly.
* Senior management (Department Head / Delivery Head) should address ‘Information Security’ during their interactions with the users.
* Posters and hand-outs may be used to create security awareness among employees.
* The Induction training for all new joiners should cover a session on introduction to Information Security Practices.
* Training should cover the following topics, but not limited to
  + Basics of Information Security
  + Organizational Policies and Procedures
  + User Do’s and Don’ts
  + Disciplinary Process
  + Evaluations and suggestions should be sought after every training session
* Refresher programs should be conducted periodically by the Management Representative to reinforce security awareness.
* Information Security awareness should also be disseminated through available mediums of communication.

### Exit Procedure

* HR shall send notification via email to all concerned support teams about the resignation, suspension, or termination of services of any employee.
  + The IT Team should take the following actions, considering the notice period:
* Disable network access, mail access, and other application access
* Backup the data from the user workstation (if requested by the Department / Delivery Head) and format the machine before allocating the system to another user.
  + The administration department should collect keys, Photo ID / Access card, and any other asset in possession of the employee.
  + The HR department creates a Clearance Form on the last day of work for the exiting employee. It is the employee’s responsibility to get all the required clearances and submit them to HR for final sign-off.
  + In case of a non-voluntary exit the clearance form of the exiting employee is circulated by the HR representative. If the clearance form is not circulated on the same day, the IT team is informed to de-activate the email ID, and the Photo ID / Access card is collected by HR from the said employee and handed over to the Admin team. The Admin team de-activates the biometric access/access card of the said employee. The said employee is escorted to the reception area by the HR representative.

## User Responsibility/Accountability

### Reporting Security Incidents and Weaknesses

* Any person who becomes aware of any loss, compromise, or possible compromise of information or any other incident, that has information security implications, shall immediately report it to the Management Representative.
* Security incidents shall be documented and used in user awareness training as learning from incidents.
* Users shall be informed that they should not, in any circumstances, attempt to prove a suspected weakness. Any action in testing the weakness would be interpreted as a potential misuse of the system.

### Disciplinary Process

* A formal disciplinary process shall be established for employees violating security policies and procedures.
* HR, in close coordination with the Management Representative shall identify and communicate any prohibited conduct related to Information Security and resulting Disciplinary actions. These disciplinary actions shall range from verbal warnings and escalations to reporting managers to written warnings, fines, and, as a last resort, termination.

### Handling of Information Security Breaches

* + In case of any observed or reported breaches of the Information Security Policy, the Management Representative should update the Incident Log Book (ILB) according to the Incident Management Policy and Procedure.
  + Management Representative should handle the reported incident as per the Incident Management Procedure.
  + The following matrix suggests the possible punitive actions for various severity of breaches:

| **Sr. No.** | **Severity Category** | **Possible Punitive Action** |
| --- | --- | --- |
| 5. | Critical | Dismissal / Legal Action |
| 4. | High | Suspension / Termination of Contract / Leave Deduction / Salary Deduction |
| 3. | Medium | Warning letter |
| 2. | Moderate | Email Warning |
| 1. | Low | Verbal Warning |

* + Suggested categorization of various violations is as below:

| 1 | Making or allowing an unauthorized entry into restricted areas |  | H |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 2 | Eating or drinking in the restricted area |  |  | M |  |  |
| 3 | Smoking in the entire office areas |  | H |  |  |  |
| 4 | Unauthorized removal of IT equipment from the office premises |  | H |  |  |  |
| 5 | Theft / Loss of company property | Can range from Medium to Critical depending on the impact | | |  |  |
| 6 | Theft/loss of customer property | Can range from Medium to Critical depending on the impact | | |  |  |
| 7 | Unauthorized relocation of IT equipment inside the premises with a malicious intent |  |  | M |  |  |
| 8 | Unauthorized access/use/modification of another person’s e-mail knowingly with the intent of getting unauthorized information | C |  |  |  |  |
| 9 | Transmitting confidential or restricted company information to other parties, not in line with organization business interests or as a breach of Information Security. Reveal or publicize proprietary or confidential information. | Can range from High to Critical depending on the impact | |  |  |  |
| 10 | Sending profane, obscene or derogatory e-mails or mails with sexually explicit content with a view to harass or share contents. | Can range from High to Critical depending on the impact | |  |  |  |
| 11 | Surfing sites with obscene or porn content OR Storing / Sharing of obscene/indecent/offensive / sexually explicit content on the organization's computing environment. | Can range from High to Critical depending on the impact | |  |  |  |
| 12 | Using personal computing resources for sustained access to corporate information without explicit permission on the same from Management Representative OR  Intentional Unauthorized access to the confidential information/documents |  | Can range from Medium to High depending on the impact | |  |  |
| 13 | Use of organization logos, organization print material or any organization materials in any webpage or internet posting unless it has been approved, in advance, by organization management.  Represent personal opinions as those of organization in public forums. |  | Can range from Moderate to High depending on the impact | | |  |
| 14 | Use software files, images, or other information downloaded from the internet that has not been released for free public use (Using somebody else’s intellectual property without permission e.g. songs, movies, reports published, white-papers, etc.) |  |  | Can range from Low to Medium depending on the impact | | |
| 15 | Upload, download, or installation of any commercial software, shareware, or freeware in violation of the product copyright or in violation of the organization group's authorized software list. | Can range from High to Critical depending on the impact | |  |  |  |
| 16 | Attempt to gain illegal/unauthorized access to organization system / remote system on the internet. Attempt to inappropriately telnet to or port scan remote systems on the internet. Use or possess internet scanning or security vulnerability assessment tools, such as Nessus, SATAN or ISS etc. without the explicit permission from Management Representative | Can range from Medium to Critical depending on the impact | | |  |  |
| 17 | Manipulating / Fudging Attendance | Can range from High to Critical depending on the impact | |  |  |  |
| 18 | Unauthorized Logging into systems using another person’s User ID and Password |  |  | M |  |  |
| 19 | Tampering with computer source codes / documents; destroying/deleting / altering any information residing in a computer resource; running a malicious code which impacts business or results in loss of data or confidentiality of information | Can range from Medium to Critical depending on the impact | | |  |  |
| 20 | Intentionally misusing or damaging company property |  | Can range from Moderate to High depending on the impact | | |  |
| 21 | Having local shares on the system with Everyone Full Access |  |  |  | Mo |  |
| 22 | Virus Outbreak: Virus / Trojan found on the computer system |  |  |  | Can range from Low to Moderate depending on the impact | |
| 23 | Virus Outbreak: Virus / Trojan found on the server | Can range from Medium to Critical depending on the impact | | |  |  |
| 24 | Tailgating / Piggybacking |  |  |  |  | L |

Disciplinary action for any employee found to have engaged in misconduct shall be administered as below:

* A three-person committee comprising representatives from HR, Department/Delivery Head and Management Representative will investigate and depending on the severity and impact of the data will take an appropriate decision. For “critical severity” incidents that may lead to termination, the concurrence from the (CEO) is obtained and the same is then communicated via email to the (CEO. A three-person committee will hand over the warning letters.
* For “high severity” incidents that may lead to suspension the employee will not report to work for the number of days during the suspension. Exception would be provided depending on the work pressure based on the decision of the three-person committee.
* Repetition of three “Low severity” incidents by the same personnel would automatically raise the severity level to “Moderate”.
* Repetition of two “Moderate severity” incidents by the same personnel would automatically raise the severity level to “Medium”.
* Repetition of two “Medium severity” incidents by the same personnel would automatically raise the severity level to “High”.
* The disciplinary action will be applicable immediately after the users have undergone and completed the ISMS user awareness induction session.

# Reference Documents

* Incident Management Policy
* Acceptable Usage Policy
* Agreements
* Incident Log Book
* Incident Management Procedure
* Logical Access Control Procedure
* ISMS Overview Policy
* IT Security Policy
* ISO 27001:2013
* Statement of Application for ISO27001:2013