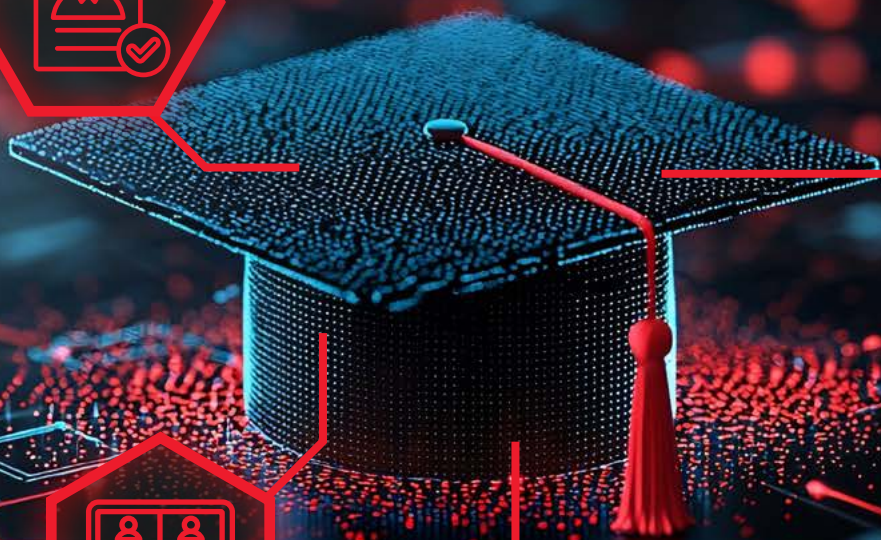
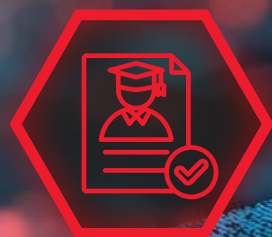


Corruption Prevention Guide on Admission of Students for Tertiary Education Institutions



5 DIGITALISED CORRUPTION PREVENTION FUNCTIONALITIES FOR ADMISSION OF STUDENTS

- 5.1 INTRODUCTION**
- 5.2 MAJOR CORRUPTION RISKS AND COMMON INADEQUACIES**
- 5.3 DIGITALISED CORRUPTION PREVENTION FUNCTIONALITIES**



5 DIGITALISED CORRUPTION PREVENTION FUNCTIONALITIES FOR ADMISSION OF STUDENTS

5.1 INTRODUCTION

In the era of digital transformation, the admission of undergraduate and postgraduate students by TEIs will inevitably undergo substantial changes, driven by advancements in technology. The integration of digital solutions minimises unwarranted human intervention, ensuring strict adherence to established procedures and requirements throughout the admission process. From online receipt of applications to information technology-assisted assessment of applications, TEIs can enhance their operational efficiency while ensuring transparency and user-friendliness in the process.

To assist TEIs in fully harnessing the advantages of utilising information technology in student admission process, this Chapter highlights relevant corruption risks, common inadequacies identified, and provides digitalised corruption prevention functionalities for the admission process.

5.2 MAJOR CORRUPTION RISKS AND COMMON INADEQUACIES

Major Corruption Risks



- ❗ Manipulation of the admission process to favour colluded applicants through manual data processing across different computer systems / modules, inadequate segregation of duties in system workflow, or ineffective user account management.
- ❗ Leakage of privileged admission information (e.g. interview / written test questions in the question bank) to the applicants due to ineffective access control in computer system.
- ❗ Corruption or other malpractices in the admission process being covered up due to lack of supervision or management oversight, ineffective information technology risk assessment and audit, absence of whistleblowing channel, or lack of digitalised functionalities in the admission process.

Common Inadequacies



- ✗ Heavy reliance on manual data processing which is inefficient and prone to human errors, due to lack of automatic data flow across different computer systems in individual schools / faculties of TEIs.
- ✗ Sensitive admission information could be easily accessed due to inadequate information security in computer system.
- ✗ Inadequate accountability and traceability of the admission process due to lax management of user account (e.g. sharing of user accounts).
- ✗ Non-compliance in the admission process due to lax monitoring (e.g. supervisors are not alerted when major steps for verification of academic credentials are omitted).
- ✗ Under-utilisation of information technology or computer-aided tools in the admission process.

5.3 DIGITALISED CORRUPTION PREVENTION FUNCTIONALITIES

5.3.1 BASIC SAFEGUARDS FOR COMPUTER SYSTEM

- Digitalise the admission process, for example –
 - invitation and receipt of applications;
 - shortlisting and assessment of applicants;
 - arrangement of interviews / written tests;
 - initial checks on academic credentials;
 - issuing of admission offers; and
 - management oversight and supervision.
- Build in security safeguards to protect the information in the computer system, for example –
 - adopt clear security classification of data / information and appropriate security measures for different classifications (e.g. access to interview / written test questions should be restricted on a need-to-know basis); and
 - build in audit trail functions for tracking access / changes to important data / information (e.g. applicants' personal data, public examination scores such as JEE scores) and review the audit logs on a risk-based approach or by way of exception reports to detect and deter any abuse (e.g. unauthorised access to privileged information, tampering of information).

- Properly manage the user accounts of the computer system, for example –
 - assign user roles based on their duties in the admission process, granting each role specific permissions to perform certain action and access on a need-to-know basis;
 - restrict the access to the admission computer system / programme to designated staff with unique login accounts and passwords;
 - promptly deactivate the user accounts when the staff have left the TEI or were no longer involved in the admission process; and
 - regularly review usage of individual user accounts to identify any irregularities (e.g. inactive user accounts).
- Provide functions in the computer system to facilitate management oversight and supervision, for example –
 - build in automatic alerts and leverage data analytics to facilitate compliance checks and detection of irregularities (e.g. expiry of student visa) such that supervisors or management could be promptly notified of any abnormal patterns or irregularities detected;
 - generate periodic information or exception reports to facilitate management oversight and alert them of possible anomalies, for example –
 - amendment of a public examination scores without justifications;
 - admission of ineligible applicants without justifications; and
 - non-compliance with the internal application processing timeframe or admission procedures.

5.3.2 SAFEGUARDS SPECIFIC TO ADMISSION OF STUDENTS

5.3.2.1 Management of Conflict of Interest

- Require all staff involved in particular admission exercises to indicate in the computer system whether they have any actual, potential or perceived conflict of interest with the applicants before they are allowed to get involved in that particular exercise.
- Automate the workflow for forwarding a declared conflict to the designated authority to determine appropriate mitigating measures.
- Use auto-matching or artificial intelligence (AI) to help match or analyse the key personnel and other particulars of applicants and those of the TEI with a view to identifying possible conflict of interest situations and detect irregularities (e.g. the name of the referee of an applicant is identical to an interview panel member).

5.3.2.2 Receipt of Applications and Communication with Applicants

- ▣ Enable receipt of applications in the computer system or web-based platform with automatic controls built in the process –
 - disallowing any alternation of application information or receipt of any new application after the application deadline;
 - maintaining audit trails throughout the receipt process; and
 - analysing Internet Protocol (IP) addresses of applicants to detect irregularities (e.g. more than one application submitted from the same IP address).
- ▣ Keep applicants informed of the updated status of their applications through the computer system or web-based platform.

5.3.2.3 Shortlisting and Assessment of Applications

- ▣ To uphold accountability and facilitate objective assessment, capture in the computer system all the scoring information throughout the shortlisting and assessment process, including the scores in the written tests or interviews by individual interview panel members and any alternation to the scores with justifications provided.
- ▣ Adopt technologies (e.g. AI) to facilitate online interviews with applicants and analyse applicants' performance.
- ▣ Enable automatic calculation of the overall combined scores, and determination of the ranking order list.

5.3.2.4 Verification of Qualifications

- ▣ Use technologies to assist the checks conducted by TEI staff, for example –
 - use facial recognition technology to compare the portraits of the applicant appearing on the application form, identity documents, academic credentials and online interviews (if applicable) to detect any impersonation or other malpractices;
 - use AI or big data technologies to detect any irregularities in the information provided in the applications and online interviews such as –
 - grammatical accuracy of the documents submitted;
 - resemblance of scores / grades attained by different applicants;
 - email domain of the referees on reference letters;
 - inclusion of AI-generated answer; and
 - similar / same typos or other mistakes made in the same batch of applications.
- ▣ Adopt technology (e.g. blockchain) to provide students with digital credentials in a secure and verifiable format for direct verification of academic credentials at the TEI's designated website / online platform.