Australian Government
Tertiary Education Quality and Standards Agency

TEQSA

TEQSA Good Practice Note: Preventing Fraudulent Documentation

Overview

Maintaining the security of certification documentation is a requirement of the Higher Education Standards Framework (Threshold Standards) 2011. Qualification Standard 2.5 states

> *The higher education provider maintains appropriate mechanisms to prevent fraudulent reproduction of certification documentation and statement of attainment documentation.*

Maintaining the integrity of student records and certification processes is essential for preserving the value of qualifications issued by Australian Higher Education providers. The validity of qualifications is relied upon by other educational institutions and employers and, as such, multiple strategies to address the risks associated with the integrity of student records and the production of certification documentation are required.

Current Practices

In relation to the production of certificates, a range of security features are currently utilised by Australian Higher Education providers to protect student transcripts from fraud including:

- Comprehensive policies and security protocols to control the storage, printing and distribution of testamurs and transcripts
- Purchase of parchment stock from reputable suppliers
- Unique security numbering of parchment stock and regular audit of the stock to ensure the use of parchment is tightly controlled
- The inclusion of security controls on the testamur including the use of: holographic image, watermark, embossed logo or seals, guilloche design, embedded watermark, wax seal or stamp, microtext, thermochromic ink, solvent sensitive or fugitive ink, blue ribbon authentication.
- Regular and ongoing staff training in the detection of fraudulent documents
- Free on-line service for third parties to verify qualifications.

In relation to the security of student record databases, management practices and security measures include:

- Staff training and awareness of potential threats
- Controlled access with real time logs and regular internal and external audits to monitor and review system access and detect irregularities
- Use of tailored security software and periodic vulnerability assessments.

Current initiatives among Australian Higher Education providers include: the electronic credentials and electronic data transfer of academic records, the development of a national digital repository of student results, and the use of secure digitally signed student documentation.

Summary

In addition to the importance of encouraging the use of free services for third parties such as employers for the verification of records and certification, current good practices by Australian Higher Education providers highlight the need for a multi-layered and coherent approach. This approach includes governance, training and effective deployment of technology to prevent fraudulent production of certification and the breach of provider record systems.