Unit of Competency

Title	Monitor data security throughout the organisation and maintain the system
Code	107035L4
Range	Protecting personal data of employees from data loss or data breach incidents. This applies to the development of routine monitoring processes with relevant stakeholders to maintain the system and data security measures to access, handle and store human resource (HR) data safely as well as archive superfluous data.
Level	4
Credit	4
Competency	Performance Requirements 1. Knowledge in the Subject Area • Understand the ever-increasing importance of keeping information and data secure and intact throughout the process of HRMS / HRIS implementation • Understand the best practices of data protection and security in HR industry in order to select the appropriate ones for the organisation 2. Applications and Processes • Complete user profiles with associated data security requirements • Coordinate with IT department to develop routine monitoring processes to maintain the system and identify necessary support for regular reviews on data security • Implement test plan on a regular basis to assess system's capability to fulfil data protection requirements defined by the organisation • Monitor security risks associated with emerging technologies (e.g. cloud-based HRIS solutions) • Coordinate with IT department or designated vendor on regular system maintenance or system upgrade for data security 3. Professional Behaviour and Attitude • Regularly implement existing security measures with IT department or designated vendor and suggest enhancement as appropriate
Assessment Criteria	The integrated outcome requirements of this UoC are: • Establishment and maintenance of data security processes and measures (e.g. a well-defined security authority matrix) based on data protection requirements defined by the organisation. • Implementation of existing security measures for identifying potential vulnerabilities and suggesting enhancement as appropriate (e.g. frequent password changes, educating employees on security protocols).
Remark	