SOP Number **202301**

Standard Operating Procedures: Faculty of Health Sciences Digital Assessments

	NAME	TITLE	SIGNATURE	DATE
Author	**GE Doyle**	**EdTech Manager (Dept of Health Sciences Education)**		**20 10 2023**
Reviewer				
Authoriser				

Enquiries: EduTech Manager (Gregory.Doyle@uct.ac.za)

Effective Date:	**Immediately**
Review Date:	**08 03 2024**

PURPOSE

This SOP provides guidelines and standardised procedures for administering and setting up online assessments within the Faculty of Health Sciences at the University of Cape Town. It applies to all staff members involved in these activities.

INTRODUCTION

This SOP is designed to provide a standardised procedure for administering and managing digital assessments within the Faculty of Health Sciences. Adopting digital assessments reflects a commitment to leveraging technology to enhance teaching, learning, and assessment processes. The rationale for this shift includes the efficiency of online assessments, potential cost savings, and the ability to offer a diverse range of question types, including multimedia items. The increased usage of online assessments necessitates a unified approach to ensure these assessments' integrity, security, and quality.

SCOPE

This SOP applies to all conveners, lecturers and staff involved in the setup, administration, and oversight of digital assessments within the Faculty of Health Sciences.

DEFINITIONS

- Assessment Owner (AO): Lecturer or convenor requesting an assessment to be created.
- Digital assessments: A formative or summative assessment delivered via Amathuba or Vula.
- Digital device: Typically, a cell phone, but it can also be a tablet or any other electronic device capable of being connected to the internet or storing information. Used to obtain a code for MFA.
- EDUTech: Staff from the EDUTech Division based in the Department of Health Sciences Education are responsible for administering and supporting online assessments.
- EOB: End of Block assessments, typically found in MBChB Years 4 to 6 courses.
- EOS: End-of-Semester assessments, which could include end-of-year assessments written by either a semester or year course. These assessments are more extensive than the end-of-block (EOB) assessments written during clinical years.
- ICTS: Department of Information, Communications and Technology Services. The central IT unit of UCT is responsible for all hardware and software.
- LMS: Learning Management System, Vula (currently MBCHB Years 4-6) and Amathuba (AHS and MBCHB Years 1-3).
- MFA: Multi-Factor Authentication – the process users go through when logging into a UCT system using their UCT username and password. A code is sent to their digital device or generated via an authentication app on a mobile device, which the user must enter to finish logging in.
- Online Assessment: A digital assessment.
- TAP: Temporary Access Password, an alternative code provided than what a user will typically receive
- during the MFA process on their digital device.

PREREQUISITES

Understanding of the UCT Examination Policy Manual, including sections related to online assessments. Familiarity with the learning management systems used at UCT, including Vula and Amathuba, and its assessment tools. Necessary training provided by EDUTech for creating and managing online assessments. Familiarity with UCT's multi-factor authentication (MFA) process and its implications for online assessments.

TRAINING AND SUPPORT

EDUTech can provide the necessary training to staff on different question types and assist in authoring, publishing, and extracting results from online assessments.

RESPONSIBILITIES

EduTech Division

- Provide training and support for staff on creating, publishing, and managing online assessments.
- Assist with authoring, publishing, and extracting results from online assessments and communicate fully with the assessment owner to ensure they are informed at every step of the process.
- Ensure secure delivery of online assessments by implementing necessary security measures (See Appendix B).
- Provide technical assistance during online assessments.
- Make all due effort to ensure assessments are set up and run securely.

Assessment Owner

- Ensure proper formatting and timely submission of assessments. Ideally, 5 – 7 working days before the assessment to EDUTech if you need any assistance.
- To provide all the necessary information required by EDU staff to set up the assessment. Assessments should not be emailed but submitted via the EDU Dropbox Vula site. Encrypting Word documents adds a layer of protection.
- The assessment owner or representative ensures the required computer lab(s) are booked and confirmation is received. Unless by **prior arrangement**, technical (IT) support is available from 08h00 to 16h30, and EDUTech (Vula and Amathuba), 08h00 to 16h30, Monday to Friday.
- Coordinate invigilation of online assessments as per the UCT Examination Manual.
- Provide feedback to EDUTech on the service received.
- Adhere to the security measures outlined in this SOP.
- Communicate with students regarding the requirements related to Multi-Factor Authentication. If students require assistance because they cannot access their digital devices, the invigilator can request TAP assistance and complete the form as per Appendix C.

Computer Lab Administrator

- Ensures that the required working computers are available and prepped before assessment(s).
- Respondus Lockdown Browser is available and updated.
- Provide TAP support during working hours only, unless by prior arrangement.

SPECIFIC PROCEDURE

Pre-Assessment Preparation

- The Assessment Owner will provide EduTech with all the necessary information and files to set up their assessment. The form, as in Appendix A, should accompany each evaluation. Where the AO sets up the assessment themselves and only requires partial assistance from EduTech, the form should accompany the request.
- EduTech will configure the online assessment settings according to the guidelines provided in Appendices B, ensuring security measures and technical requirements are met.

Setting up the Assessment

- If required, individual questions will be automatically shuffled. By default, the order of MCQ options will be shuffled if pedagogically appropriate.
- Courses with a separate assessment site will be unpublished except for the assessment duration.
- AO will be asked to check each assessment before publishing it, after 2-5 working days of sending said assessment.
- EDUTech will publish the assessment on the LMS after approval from the AO.

Multi-Factor Authentication (MFA) for Online Assessments:

In 2023, ICTS (Information & Communications Technology Services) enabled MFA to boost the security of UCT accounts and online services, including Amathuba & Vula. AO should emphasise preparedness, ensure they bring the digital device with them, do timely SIM swaps, and visit ICTS for number changes. Suppose a student does not have access to their digital device before an assessment. In that case, the Computer Lab

Administrator can assist them by issuing a temporary code after verifying their student ID and having the invigilator complete the TAP Request Form.

Security Measures

- Use the Respondus Lockdown Browser.
- Implement password protection, use groups, and lockdown browser settings for the assessment.
- Ensure proper invigilation as per UCT Examination Manual guidelines and ensure identification of students, including following guidelines for recording student attendance and restroom use.
- Afterwards, collect scrap paper provided to students.
- Once an assessment is completed and submitted, students must log off the LMS, turn off the computer, and leave the computer lab.
- Once students have logged in using MFA, the Chief Invigilator must ensure their digital device is not at their computer or person.
- CCTV cameras have been installed at the Health Lab and Wolfson Lab. Depending on which computer is under scrutiny, it might be possible to obtain footage related to breaches of assessment policy. There are only a limited number of cameras, which do not cover every square meter in detail, stored for seven days, only available on request, and viewable from the Computer Lab Administrator's PC. Contact the EDUTech Manager for additional information.

Delivery of Assessment

- By request, EDU staff members will be on hand for the first and last 15 minutes of any assessment unless other arrangements have been made. The staff member will be on standby for the rest of the evaluation.
- The Chief Invigilator should ensure adherence to UCT Examination Manual rules.
- Provide necessary instructions to students at the start of the assessment.
- Implement procedures for collecting attendance slips, checking student IDs (Identification Documents), and monitoring restroom use.
- Maintain vigilance throughout the assessment, with invigilators moving around the room.

Impact of MFA

Due to students needing access to their digital devices at the start of any online assessment while adhering to the rule of not having any electronic device with internet access or recording ability in their person, the following are recommended.

- Ensure students are in the venue at least 15 minutes before the start of the assessment to enable them to log in using their digital devices.
- Students who require assistance via TAP because they no longer have access to their digital devices need to see the computer lab administrator before the assessment starts with some form of photo identification (student card, ID, Driver's license). The invigilator needs to complete a form to obtain a temporary code.
- Students arriving late for an assessment and needing MFA assistance may have their assessment time cut short. The Chief Invigilator must decide if these students will be given the full duration designated for the assessment, or finish when the computer lab reservation comes to an end. Depending on if there are other bookings following this assessment.
- Students must enter the computer lab and either fill out the smallest venues first or, if in a larger venue, fill out the venue from the row furthest from the entrance. This should minimise students returning to their bags to put away their digital devices after using MFA.

If any assessments start after regular working hours, 4 pm, and students need TAP assistance, they must see the Computer Lab Administrator before 4 pm. They will receive a temporary code, which will be valid for 4 hours. The code can only be used once, i.e., students should not use it to log in to check their email.

Post-Delivery of Assessment

- EduTech will provide standard reports and analyses within 24 hours after the assessment.

- EduTech will assist in retrieving and analysing assessment results, adjusting scoring, and marking as requested.
- Regrading of MCQs is possible, but not the other question types. Any question's score can be set to 0, i.e. "removed from the assessment".
- AO are encouraged to study the item analysis produced by Vula or Amathuba. Consider questions with negative discrimination and the distribution of questions flagged as difficult or easy.

SOP VIOLATIONS

AO must adhere to the SOP, comply with security measures, and take cognisance of MFA; otherwise, EduTech cannot be held responsible for anything that goes wrong before, during, or after an assessment.

FORMS/TEMPLATES TO BE USED

- Assessment Setup Information: The assessment owner needs to fill in the details of the assessment. The online form is available here.
- TAP Request Form: Available from the desk at Health Lab or Wolfson.

INTERNAL AND EXTERNAL REFERENCES

- ICTS website for more information on MFA at UCT, FAQs, and recommendations for managing
- accounts securely.
- UCT Examination Policy Manual

CHANGE HISTORY

APPENDIX A – ASSESSMENT SETUP INFORMATION
APPENDIX B: RISKS TO BE CONSIDERED FOR ONLINE EXAMINATIONS

Before examinations

- Inappropriate technology choices/lack of awareness of risks.
- Incorrect setup of online examinations (e.g., to reveal answers)
- Disclosure of examination questions (e.g., a lecturer's or administrator's PC being compromised by spyware/malware/phishing, network security being compromised by password disclosure, or material being placed in an insecure online location)

During examinations

- Access to supporting content (e.g., LMS, PC, internet).
- Communication with others (e.g., Chat, SMS, Instant Messaging) from a PC or digital device.
- Leaking examination password (allowing examination to be taken online outside the examination venue).
- Recording the examination questions for subsequent "underground" circulation (cut & paste to desktop/flash drive/online location).

Security factors to consider for online examinations.

- Designing the examination appropriately to minimise the scope for cheating. Randomised questions and answers (each student have a different order of questions and presents answers randomly).
- Password restrictions for each examination (what you know).
- IP-based restrictions for each examination (where you are).
- Restrictions on the Windows desktop and browser in the lab during the test (e.g., no ability to run other programs).
- Restrictions on the network configuration for the lab during the test (e.g., no external Internet access).
- Time pressure.
- Analysis of results.
- Detailed activity log on Vula (later doing forensic auditing if required).