ΠΑΡΑΡΤΗΜΑ ΙΙΙ
Αδιάβλητο & αξιοπιστία εξετάσεων

Οι κυριότερες σχετικές ασφαλιστικές δικλίδες και τα μέτρα που θα εφαρμοστούν ενιαία για το αδιάβλητο και την αξιοπιστία της διενέργειας της εξέτασης με τα μέσα εξ αποστάσεως αξιολόγησης έχουν ως εξής:

1. Η διαφάνεια της διαδικασίας διασφαλίζεται από το γεγονός ότι οι φοιτητές/τριες παρακολουθούν τη διαδικασία όντας/ούσες συνδεδεμένοι/ες με εικόνα και ήχο καθ' όλη τη διάρκεια της εξέτασης, ενώ ακόμη και στην περίπτωση της προφορικής εξέτασης ολιγομελών ομάδων φοιτητών/τριών, η εξέταση με εικόνα και ήχο γίνεται με την ηλεκτρονική παρουσία συμφοιτητών/τριών ή/και επιτηρητών.
2. Ο έλεγχος της ταυτότητας των εξεταζόμενων διασφαλίζεται από την αντιπαραβολή της φοιτητικής τους ή άλλης επίσημης ταυτότητας με το πρόσωπό τους, όπως εμφανίζεται στην κάμερα κατά τη διάρκεια της εξέτασης, σε συνδυασμό με το σύστημα αυθεντικοποίησης των ιδρυματικών λογαριασμών των φοιτητών/τριών.
3. Το αδιάβλητο της εξέτασης διασφαλίζεται από τις μεθόδους εξέτασης, σε συνδυασμό με τη δυνατότητα συμπληρωματικής προφορικής (εξ αποστάσεως) εξέτασης, στην περίπτωση της γραπτής εξέτασης.
4. Σε κάθε περίπτωση ο/η φοιτητής/τρια καλείται να δηλώσει ότι συμμετέχει στην εξέταση και ότι κατά την διάρκεια της εξέτασης δεν θα έχει οποιαδήποτε συνομιλία ή με άλλο τρόπο επικοινωνία, ανταλλαγή αντικειμένων ή οποιαδήποτε συνεργασία με άλλο άτομο, και δεν θα αξιοποιήσει οποιαδήποτε πηγή βοήθειας που δεν θα προβλέπεται από τον/την διδάσκοντα/ουσα (βλέπετε αναλυτικότερα Παράρτημα ΙΙ).
5. Η ασφάλεια του συστήματος και των πληροφοριών που συλλέγονται διασφαλίζεται με βάση τα μέτρα ασφάλειας που λαμβάνει η Κεντρική Δ/νση Πληροφορικής και Επικοινωνιών. Τα συστήματα MOODLE, Open eClass, BigBlueButton (BBB) φιλοξενούνται στους εξυπηρετητές του Ιδρύματος και τα διαχειρίζονται, αποκλειστικά και μόνο, μέλη του προσωπικού του Ιδρύματος. Πρόσβαση στο Zoom θα δίνεται μέσα από τους Ιδρυματικούς λογαριασμούς των χρηστών. Η Κεντρική Δ/νση Πληροφορικής και Επικοινωνιών έχει λάβει όλα τα απαραίτητα τεχνικά και διοικητικά μέτρα για την προστασία των παραπάνω συστημάτων και των υποδομών που τα υποστηρίζουν από απόπειρες παραβίασης, ενώ η πρόσβαση στα συστήματα αυτά γίνεται μέσω ιδρυματικών λογαριασμών χρηστών, με βάση το ιδρυματικό σύστημα αυθεντικοποίησης και διαχείρισης δικαιωμάτων πρόσβασης.