The following are recommended exam security practices that may be used in addition to deploying the IP restriction tool in an exam in eCampus:

1. Use Respondus LockDown Browser and require a password to enter the exam.
   The LockDown Browser adds a layer of protection preventing users from accessing websites and other applications that could compromise the testing environment. **NOTE:** Exams requiring the LockDown Browser will automatically have a password set. Changing or removing the password will allow users to take the exam outside of the LockDown Browser.
2. Provide a disclaimer as the first question of every exam. Example Below:
   I hereby acknowledge this exam is to be completed only in the designated proctored computer lab. By continuing with the exam, I am verifying that I am in the designated proctored computer lab. I understand that failure to take the exam in the designated area will be considered as cheating and reprimanded according to University policy.
3. Create multiple exams and use Adaptive Release to release specific exams to specific groups of users. Test Availability Exceptions may be used to provide customized exam availability and duration to specific users.
4. The password can be changed after each exam. However, changing or removing a password is not recommended in cases where the LockDown Browser is enabled.
5. Use a paper copy of the exam for questions only and then use eCampus as an electronic scantron where students will note the answers.
   Example: Create an assignment with X questions. Include no text in the questions or answers except the following:
   a. Question 1
      i. Answer A
      ii. Answer B
      iii. Answer C
      iv. Answer D

   They will select their answer based on what they read in the paper exam. On their way out of the lab, students need to turn in the paper exam to get checked off the attendance list.
6. Compare the attendance list created during the exam to the list of students in the course.