Updated Guidance

First Published: 08 Apr 2020; Last Updated 27 Apr 2020

Version: 1.3

Proctorio Remote Proctoring Solution

Overview

This document is an assessment of the proposed remote invigilation tool Proctorio. The ANU Information Security Office initially provided a quick assessment based on publicly available documentation. This document supersedes the previous guidance and uses information based on own ANU's ongoing analysis of Proctorio, independent reports, interviews with company representatives and other verifiable online material.

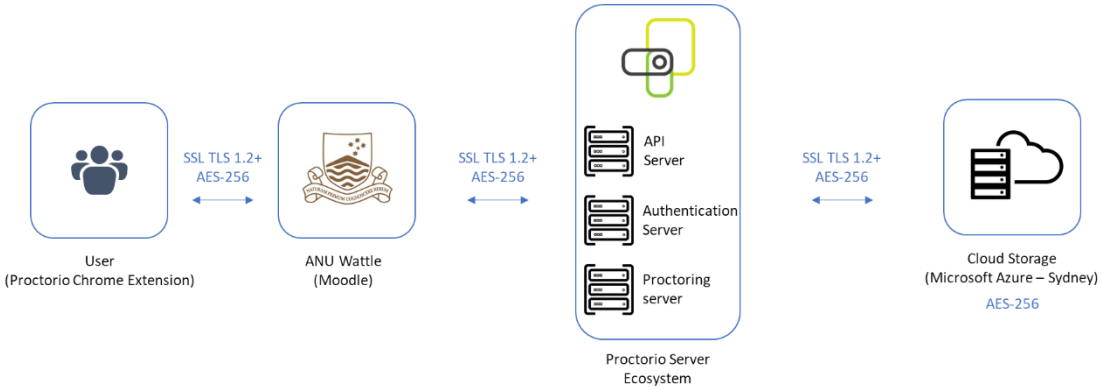
Providing a security assessment is standard practice before the acquisition of any system or service which may hold ANU data, integrate with ANU systems or contain Personally Identifiable Information (PII). There is, however, one notable difference for this assessment. Given the high level of concern and interest expressed by students and staff, in the interests of transparency, this document contains more contextual information than usual.

This document is intended to complement the Privacy Impact Assessment (PIA) provided by ANU's Chief Privacy Officer. It is recommended that this document be read in conjunction with the PIA.

This document provides information that the Information Security Office has at the time of release. The assessment of Proctorio is currently ongoing. So this document will be updated until all security aspects have been covered to ANU's satisfaction that there are no information security risks to the system's users. We encourage users of this document to regularly check the ANU website for updates to this document.

How does the Proctorio system work?

A simplified overview of how Proctorio works is captured in the diagram below.



The security assessment being undertaken by the ANU Information Security Office covers the Proctorio browser extension, ANU Wattle, the transport protocol in between each component, the Proctorio server ecosystem and the cloud storage used to hold recorded exam sessions.

Proctorio uses a Google Chrome extension installed by the test taker. The user then logs into the Wattle site, using the usual authentication process, which has been configured to recognise the Chrome extension. Wattle, in combination with Proctorio, is then able to remote proctor the session using the user's video camera, microphone, keyboard and screen.

Wattle communicates with the servers within the Proctorio ecosystem which enables Wattle to authenticate itself, access the Proctorio API and commence the capture of the video session. Via the API server, Wattle can access the cloud storage in Microsoft Azure (Sydney) where the session data will be recorded.

An examiner logs in to the above ecosystem, via Wattle's grade books, and can decrypt and replay the recorded session.

What does Proctorio capture from a student's computer?

Based on information from Proctorio's documentation and ANU's assessment of a live test the Information Security Office has been able to ascertain that the following information can be captured during the examination period:

- Recording of video. From this video, Proctorio can capture and if needed note head, eye and mouth movements.
- Recording of audio
- Recording of the student's screen
- Scan the environment/room of the test taker – this is a 15-second scan if required.
- Key presses
- Mouse movements
- Attempts by the user to use the right click functionality
- Efforts by the user to use cut and paste functionality
- Attempts by the user to print or download material
- Attempts to resize the browser, open new tabs/windows or navigate away from the exam environment.
- Record URLs visited during the exam session.
- Detects, before examination commencement, if the user's computer has more than one monitor – this information is not captured; it is a detection routine before the examination.

The above indicates what can be captured and to what degree the examination environment is locked down. In practice, it is up to each examiner to choose what subset of information is needed and therefore collected. The degree to which each indicator is

flagged by Proctorio is also determined by the examiner and can be adjusted as required pre- and post-exam.

ANU is working with Proctorio to get a copy of the metadata payload used when capturing the above information. With Proctorio's permission, ANU will provide this to students and examiners in the interests of transparency. Once the payload is available, this document will be updated.

How does Proctorio flag unexpected behaviour?

Depending on the settings chosen by the examiner the Proctorio system will "flag" any activity by the test taker which the examiner would deem to be unusual given the nature of the test. The sensitivity with which the system flags is also set by the examiner. For example, a short multiple-choice quiz may have high sensitivity for head/eye tracking and key presses but may disregard (and therefore not capture) other information. Conversely, an open book exam may have little or no sensitivity for eye-tracking because it is expected that the test taker will frequently be looking at notes and books.

There is a relatively basic algorithm which reflects what information is captured and the sensitivity settings determined by the examiner. The system will flag anything outside expected behaviour on this basis and highlight it for the examiner during the exam replay. The system itself does not determine if any cheating behaviour has occurred – that is at the sole discretion of the examiner post-exam using information from the Proctorio recording.

Why might information be collected?

Broadly, the capabilities of the system are designed to mimic or provide a proxy for normal face-to-face invigilation. That said a notable difference is that the checks usually done before or during a face-to-face exam, e.g. validation of identity, is done post-exam by the examiner. These are digital equivalents of integrity checks and standardised environments used in most exams and adjusted to create an equal footing for all students for a range of home environments.

Below is a summation of why each captured piece of information may be needed by the examiner:

- **Facial captures** occur at the beginning of the test. In essence, this is used to validate the identity of the student taking the exam. A webcam shot of the student's face and ID card are captured so that the examiner can verify the student post-exam. There is no facial recognition in use.

- Screen captures can be used to take video screenshots of the student's desktop. This is to ensure there is no unauthorised material present on the device being used to do the exam. A maximised browser screen will mean that is all Proctorio will capture. The scope of the screen capture is determined by the examiner in advance and the test-taker is informed at the commencement of the exam. All material within the scope of the screen capture can be viewed by examiners, even if

that material is private to the test-taker. Students should ensure that private material is not displayed within the scope of the screen capture.

- **Room scanning** is done so that the student can validate that they are taking the exam by themselves so the examiner can to some degree standardise. For exams where this has been activated, the student is asked to do a 15-second sweep of their test environment. Depending on the settings used by the examiner, the student may be asked to repeat this process if more than one person is detected in the room, e.g. multiple voices or multiple faces

- **Video capture** provides a range of capabilities. Head and eye tracking are used to determine the degree to which a student is looking at the screen. Mouth tracking is used (in conjunction with voice) to determine if a student is talking to someone in the exam environment. Video capture also detects if a student has left the exam environment unexpectedly or if there are multiple faces present.

- **Voice capture** is used to detect multiple voices.

- **Key presses** are used to detect keyboard activity if such activity is not expected. Proctorio does not capture the content of what is typed, i.e. keylogging.

- **Mouse movements** may be captured to determine on-page navigation or if the user has navigated away from the exam environment.

- **URL recording** is used to ensure (if required) that students do not use unauthorised online material.

- **Single screen checks** are used to ensure that multiple screens can not be used to circumvent exam controls, e.g. streaming answers or course content on a second screen.

- **Browser and system functionality controls** are designed to temporarily lock features which may not be allowed during the exam or may impact the integrity of the exam process. These may include cutting and pasting. Proctorio effectively blocks “write to clipboard”. Right-clicking can be blocked for similar reasons. Printing and downloading may be blocked to reduce the chance of unauthorised material being introduced or exam material being transmitted. The plugin will also clear the browser cache used during the exam period but nothing beyond this.

- **User navigation controls** like new windows, browser tabs, and navigating away from the exam environment may be monitored and flagged if this is not expected behaviour. This is designed to ensure test takers stay within the approved exam environment and not able to access external information.

What is not collected?

- There is no indication that private information is captured by the system. It worst it may be the inadventant capture, through the webcam or screen, of information the test taker may not want captured. This information is only accessible to the examiner and usually within the control of the test taker to make sure such information is not visible.

- Proctorio does not access files on the student's hard drive, read emails or other data on the computer it is installed on. At most, it writes to the browser cache during the exam period and deletes the files it creates at the end of the exam. The extension can only be installed with user consent and readily uninstalled without leaving any residual files.

- Proctorio does not use facial recognition. The resolution that it is tuned to use (irrespective of the user's webcam capabilities) is 320x240 pixels. This is a relatively low resolution that is not overly suitable for accurate facial recognition.

- Proctorio does not utilise any form of biometrics. All potentially-biometric information (such as voice and video) transmitted to Proctorio servers is cryptographically protected from Proctorio and from public access. It is only available to ANU staff for the purposes of the exam.

Security assessment of the Proctorio transport protocol and encryption.

Data-in-transit: ANU has undertaken a series of tests against the servers intended to be used by Proctorio for ANU exams using www.ssllabs.com and assessed that they are suitable to transmit and store ANU information. The links between each system component utilise Transport Layer Security (TLS) version 1.2 or 1.3 utilising the AES-256-GCM encryption algorithm. This is one of the highest standards for transmitting data securing across the internet and comparable to systems used by banks. The encryption keys are generated on the fly and are not subject to man-in-the-middle attacks. In other words, only data collected during the exam cannot be intercepted and decrypted by an unauthorised third party or Proctorio. It is in this respect, analogous to an online banking session.

Data-at-rest: All data captured from the exam period is stored in a Microsoft Azure cloud instance hosted in Sydney. The data is encrypted as it is stored using AES-256 encryption. The keys and secrets to access this data – usually through a replay of the recorded exam – is stored in Wattle and only accessible by the examiner.

Security assessment of the Proctorio Chrome extension.

The assessment of the Chrome extension used by Proctorio is ongoing. The ANU Information Security Office is working with Proctorio to get a copy of the extension's source code. Resources specialising in Chrome extension design and security have been identified for the source code review. ANU has already noted Proctorio's use of the WebRTC library (which may introduce a vulnerability depending on how it is implemented) and has asked Proctorio for clarification. This document will be updated once the review is completed.

Security assessment of Proctorio's server and web infrastructure.

Proctorio has provided a recent detailed penetration and vulnerability assessment which has been reviewed by the ANU Information Security Office. Based on this review, there are were no security issues of either high or medium severity. The low severity issues are not likely to result in unauthorised access or data loss. Proctorio also provided details of a recent security assessment done at another higher education institution. The reports, like many penetration testing reports, itself contained commercial-in-confidence data and was released to ANU under a non-disclosure agreement. So, it is not possible to release this information.

That said Proctorio allowed for the release of its responses to the ANU's standard security questionnaire, regarding is security protocols and design, as well as its responses to the Higher Education Community Vendor Assessment (HECVAT) compliance questionnaire (https://library.educause.edu/resources/2020/4/higher-education-community-vendor-assessment-toolkit).

Proctorio's answers will be made available on the same website as this document.

Based on the responses given by Proctorio about its security protocols, the independent security reports and ANU's own analysis it is assessed that Proctorio's server infrastructure does not pose any security risk to our test takers.. If any information comes to light that Procotorio's security posture was comprmosied, ANU would re-assess its security advice and ongoing use of Proctorio.

Security assessment of Wattle.

The Proctorio solution relies heavily on ANU's Wattle (based on the Moodle version 3.5 learning management system) site. As such the over all security assessment is contingent on how secure Wattle itself is. The site is quite secure and was not impacted by the 2018 data breaches. However, the ANU Information Security Office is working with ANU ITS to review all security settings, and where needed further strengthen the system and introduce two-factor authentication for examiners. This document will be updated to reflect changes to Wattle once the assessment and remediation is completed.

Security assessment of Microsoft Azure (Sydney).

As with all cloud providers providing services to Government clients, Microsoft Azure has undergone a rigorous review by an independent auditor. This review known as System and Organisation Controls (SOC) report has been provided to ANU for review. This report covers privacy, confidentiality, processing integrity, availability and security aspects and is an important report to receive when evaluating a vendor. Based on the information contained in the SOC reports ANU has received regarding Microsoft Azure we deem the there is very little risk of data loss with respect to exam data stored using this service. As noted in this report, the data held on Azure is encrypted using AES-256 with ANU holding the only keys.

Other security considerations.

Comparisons with ZOOM security issues: The ANU Information Security Office has provided an in-depth security assessment on Zoom, which can be found here: https://services.anu.edu.au/information-technology/software-systems/anu-zoom-client. ANU has found no significant concerns Zoom noting that the university uses an AARNet on-premise instance. The vendor has patched recently disclosed vulnerabilities; and ANU's ZOOM privacy and security settings. Zoom will continue to be evaluated by the ISO as new information comes to light. That said, there is no overlap between Zoom and Proctorio and their respective security infrastructure.

ANU Security incidents: Understandably staff and students will have concerns in the wake of ANU's data breaches in 2018. While there is still much to do, ANU continues to invest significant resources towards improving its security posture. ANU now has in place a strategic information security program that will run across four years and a dedicated information security workforce.

Proctorio is a software-as-a-service offering, meaning that it is hosted outside the ANU's network in a Sydney based data centre. As such it there is no relationship between ANU's network security and Proctorio's infrastructure other than Wattle integration – already covered in this document. As noted elsewhere in this document, ANU's Wattle infrastructure or data was not compromised by the data breaches.

Data security controls and standards: Proctorio has provided details on how security controls were implemented using appropriate controls in line with a range of well-regarded international standards. These include the US Department of Defence and NIST 800-171. The controls also satisfy DFARS and ITAR requirements. Also, Proctorio complies with the following regulations and certifications: EU GDPR (General Data Protection Regulation), FERPA (Family Educational Rights and Privacy Act), COPPA (Children's Online Privacy Protection Act), CSPC (California Student Privacy Certified). Australia does not have data protection legislation directly comparable to GDPR. Instead, we rely on the principles contained in the Privacy Act 1988. ANU must accord with these principles, and the assessment for this is included in the PIA. It should be noted that EU GDPR is one of the most stringent data protection laws.

The Information Security Office will engage an independent assessor to provide an assurance report that the data held on the Microsoft Azure servers has been deleted once the examiners deem they no longer need the data.

Privacy: Proctorio has been recognised by the Internet Keep Safe Coalition for meeting rigorous "test-taker data and privacy standards". Only privacy trained authorised staff can unlock and view the exam recordings, not Proctorio. Please refer to the PIA for more details on privacy.

Personal Information Disclosure: There is no evidence that the information collection, will in any way be available to "another agency, a contractor, the private sector or to the public".

Summary Assessment

As noted in the overview this security assessment is ongoing. That said the information we have received to date along with ANU's own analysis indicates that the cybersecurity risk to ANU, our systems and most importantly our students is very low. We will continue to update this document as more information comes to light.

Some usage considerations.

Student using Proctorio for exams may wish to apply the following usage and security prototocols:

- Always have up to date software on your exam machine. These include your Chrome browser, operating system and any other applications on your device.
- Have some form of security software on your device.
- Consider creating a separate account on your device for the exam. This is particularly important if using a shared device or one that might be used for work as well as study,
- Consider maximising the browser during the exam if there are concerns regarding screen capturing the desktop. Proctorio will only capture what is on the screen.

An invitation to hack Proctorio.

ANU's newly formed Information Security Office, formed in the wake of the data breaches, is staffed by a number of experienced practitioners drawn from industry and Government security agencies. We are always looking for ways to test and re-test our systems as new threats emerge or new ways to compromise systems are found.

So, our professional curiosity drove us to ask Proctorio if they were willing to allow us to conduct a a security test against their infrastructure. Surprisingly they said yes! Work is now underway to find a suitable time and place to undertake this event.

If you are a student and you have persevered reading this document up to this point, given the high level of interest in Proctorio the ANU Information Security Office and the Office of the Vice-Chancellor would like to make an open invitation to you and to any ANU student who would like to participate individually or as a team to test Proctorio's defences. We are also offering a prize of computer equipment worth up to $10,000 for any team or individual who can demonstrate a weakeness in Proctorio's security.

The Proctorio instance will be a test environment set up to mirror our own but not contain any sensitive information or cause any impact to Proctorio's other clients. ANU does not sanction, encourage or support anyone trying to circumvent the defences of Proctorio's systems outside the controlled environment we will set up for the purposes of this event.

In addition, any team or individual who can either break Proctorio's security or demonstrate a high level of skill and aptitude during the hack-a-thon will be offered a job in our new Cyber Integration Centre which will open later this year. For more details please email us at CISO@anu.edu.au.

About us

The ANU Information Security Office was stood up in March 2020 and was formed in the wake of the 2018 data breaches and is one of a number of strategic initiatives created under four-year uplift of ANU's information security, which commenced this year. Later this year the Office will supersede the current ITS IT Security capability – which will be merged with the Information Security Office. The Office will be based in the Cyber Integration Centre, which is currently being fitted out. The Information Security Office works closely with the ANU Cyber Institute, a range of strategic industry partners and Government security agencies. The Office reports to the Chief Information Security Officer and is responsible for all aspects of information security across campus.

ANU Information Security Office
CISO@anu.edu.au
The Australian National University
Cyber Integration Centre
Canberra ACT 2601 Australia
www.anu.edu.au

CRICOS Provider No. 00120C