The use of AI tools in our security operations help monitor our systems activity and alert of potential threats, such as unusual logins, out of the ordinary network traffic and file transfers that look suspicious. When an alert is triggered, it will include an explanation for what has happened to trigger it and why.

A security analyst would be trained and in the loop, letting them review, confirm or override the alerts. If you believe the alert is incorrect, you may submit an appeal with the help desk. All appeals will be reviewed within a week of submission and a written response will be provided.

Only the minimum and necessary data will be collected needed for threat detection. All sensitive information will be redacted and the data that is kept will be retained until investigation is complete.

Our AI system will be retrained quarterly and the policies will be reviewed twice a year to ensure reliability and transparency. We will track how accurate the system is, how many false positives it detects and response time.