Access Control Policy
Employee contracts
Review footage before release

Threats
- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
- External attacker linking footage to real identity

Threats
- External attacker launching DoS against cloud storage infrastructure
- External attacker launching DoS against cloud storage itself
- External attacker gained admin rights to code repository
- External attacker gaining admin rights to cloud storage

Threats
- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
- External attacker/malicious insider tampers with source code
- External attacker/malicious insider tampers with saved information
- Also consider compliance with legislation
**Access Control Policy**
- Employee contracts
- Review footage before release
- Review relevant legislation

**Threats**
- External attacker impersonating user to access app
- External attacker modifying saved information
- External attacker intercepting traffic to modify information
- External attackers linking footage to real identity

**Threats**
- External attacker launching DoS against cloud storage infrastructure
- External attacker launching DoS against cloud storage itself
- External attacker gained admin rights to code repository
- External attacker gaining admin rights to cloud storage

**Threats**
- External attacker impersonating staff to access code repository
- External attacker impersonating staff to access cloud storage
- External attacker/malicious insider tampers with source code
- External attacker/malicious insider tampers with saved information
- Also consider compliance with legislation
TAKING THIS FURTHER

- These are basics
- Need to go lower
  - Technology
  - Protocols
    - How can each functionality be abused?
- How can attackers bypass the controls we already have?
- Make threat modelling iterative
- Assign responsibility
IF YOU KNOW NOTHING...

- What are we building?
- What can go wrong? STRIDE
  - Spoofing
  - Tampering
  - Repudiation
  - Denial of Service
  - Elevation of Privileges
- What are you going to do about it?
- This is the beginning but not the end
RESOURCES USED

- Threat Modelling with STRIDE adapted from Threat Modelling: Designing for Security (Wiley, 2014) by Adam Shostack
- https://docs.microsoft.com/en-us/previous-versions/msp-np/ff649749(v=pandp.10)
- Walkthrough: Creating a Threat Model for a Web Application