**Threat Modeling for SaaS Applications**

The following list of entity controls initiates the process starting the threat identification and covering the minimum standard for threat modeling a SaaS application.

|  |  |
| --- | --- |
| **Entity Controls** | **What can go wrong?** |
| Responsible for establishing policies and procedures related to information security. | If security policies are not appropriately set, an inside threat (authenticated user) may be able to exfiltrate data. |
| Establish logical access controls for user provisioning, role-based access, user de-provisioning, and user access reviews. | If access control policies are not set correctly, an authenticated user may have access to data outside their role and may be able to delete files accidentally. |
| Responsible for establishing robust authentication protocols. | If multi-factor authentication protocols are not set up correctly, threat actors may be able to access restricted company resources. |
| Responsible for the timely termination of user accounts. | If user accounts are not terminated in a timely fashion, former employees may be able to access company data. |
| Responsible for change management processes within an application. | If change management procedures are not set, followed, and communicated to all individuals, environmental changes may cause service disruptions. |
| Responsible for configuring data storage, archival, and retention requirements within the SaaS product. | If data storage requirements are not appropriately set, data may be improperly removed once a set capacity is met.  If archival and retention policies are not set correctly, important regulatory data may not be available during upcoming audits or compliance reviews. |
|  |  |