A6: Security misconfiguration

Here are some specifics:

* Be consistent among company departments. Configure common apps identically with strong separation between application architectures. Development, production, and quality should be configured so that data can be accessed as needed, but with individualized passwords and user accounts. This promotes security, accountability and helps trace errors back to particular departments and users.
* Disable company server directories, archive or delete old files, and get rid of unneeded services. This includes disabling or deleting sample apps that come with your app servers. Also modify your app servers default mode regarding returning user traces to users with error information that they might not understand, but an attacker would.
* Remove old privileges and user accounts.
* Update individual software security patches, update legacy systems, get rid of orphaned custom code.
* Make sure all mobile device defaults are changed accordingly.
* Immediately change new employee defaults and delete terminated employee user permissions and accounts. This includes mobile devices and cloud access.
* Monitor outside vendor cloud usage of company data.