Security of CAST Managed Services

Overall security measures

CAST cares a great deal about security.

Since 2015, CAST has maintained **ISO 27001** certification for the following activities:-

- Development
- Quality Assurance
- Release management
- Operating and Facilities management

All developers are trained in secure development practices

All software and services are regularly assessed (penetration test and audit code) by third party specialists

Keeping customer source code secure

CAST does provide a managed service that can optionally be run on CAST internal infrastructure. If a customer uses this service, they can be reassured from a security perspective that:-

- Customer source code is **encrypted** in transfer and in storage (sftp or https) and transferred through a secure web application that has been assessed (code audit and penetration test) by a third party
- File servers run in ‘blind’ mode so uploaded files cannot be seen. In addition, immediately after upload, files are automatically transferred to an **int ernal server** behind the firewall. So, even if a customer accidentally shares the account login, source code cannot be copied from the server by a third party
- Customer **data**, such as database content, is **never** requested or needed for an analysis. Only information on database structure and table size
- The account used to upload customer source is protected by a **strong** auto-generated password and created specifically for the duration of each customer project, which limits the risk of leaks
- During the analysis, customer source code is stored on a dedicated **secure server** with strictly managed access control
- Access to the dashboard with the analysis results is limited in time and restricted to **registered** accounts, and can furthermore be limited to **IP addresses**, or controlled via **LDAP** or **SAML** as requested by customers
- At the end of a project, customer data is deleted through a secured **wipe tool** (DOD 5220.22-M compliant)