Gallagher Security

Software Development Lifecycle & Data Protection

Copyright © Gallagher Group Limited

Disclaimer

This document gives certain information about products and/or services provided by Gallagher Group Limited or its related companies (referred to as "Gallagher Group").

The information is indicative only and is subject to change without notice meaning it may be out of date at any given time. Although every commercially reasonable effort has been taken to ensure the quality and accuracy of the information, Gallagher Group makes no representation as to its accuracy or completeness and it should not be relied on as such. To the extent permitted by law, all express or implied, or other representations or warranties in relation to the information are expressly excluded.

Neither Gallagher Group nor any of its directors, employees or other representatives shall be responsible for any loss that you may incur, either directly or indirectly, arising from any use or decisions based on the information provided.

Except where stated otherwise, the information is subject to copyright owned by Gallagher Group and you may not sell it without permission. Gallagher Group is the owner of all trademarks reproduced in this information. All trademarks which are not the property of Gallagher Group, are acknowledged.

Copyright © Gallagher Group Ltd 2024. All rights reserved.

Document History

Edition	Date	Author	Comment
1.0	1 May 2021	NW	Initial Release
1.1	4 Oct 2021	PB	Minor Revision
1.2	14 Feb 2023	NW	Updated ISMS section (1.6)
1.3	2 Dec 2024	MS	Minor Revision

Contents

1 SDLC Software Development Lifecycle 5
1.1 SDLC Overview 5
1.2 Physical Security 5
1.3 Employee Security 6
1.3.1 Hiring Process 6
1.3.2 Training Material – Security Awareness 6
1.4 Procedural Security 6
1.4.1 Access to Security Issues and Vulnerabilities 6
1.4.2 Responsible Disclosure 6
1.4.3 Password security 7
1.4.4 Code Review and Check in Policy 7
1.4.5 Release Branch Management Strategy 7
1.5 Quality Management System 7
1.6 Information Security Management System (ISMS) 8
1.7 Business Continuity Management 8
1.8 Disaster Recovery Policy 8

2 Secure Coding Standard 9

3 Configuration Management System (CMS) 10
3.1 Source Control 10
3.2 Builds 10
3.3 Build Machines 10
3.4 Work Items 10
3.5 ECN (Engineering Change Notice) process 10

4 Security Policy / Processes/ Procedures 11
4.1 Security Related Company Policies 11
4.2 Security Related Processes 11
4.2.1 Threat Modelling Process 11
4.2.2 Security Design Reviews 11
4.2.3 Independent Penetration Testing 11
4.2.4 Approach for Managing Specific Site Data 11

5 High Level Testing and Verification Approach 13
5.1 Alpha Testing Process 13
5.2 Automated Testing Process 13
5.3 Independent penetration testing 13
5.4 Software Release Process 13
5.5 Insider Program 14

6 Secure Delivery Procedures 15
6.1 3rd Party software 15
6.2 Gallagher Supplied software 15
6.3 Command Centre Cloud Infrastructure 15
6.3.1 Functional overview 15
6.3.2 Data transmission 15
6.3.3 Cloud Services 16
6.3.4 Command Centre Cloud Data storage and Approach 16
6.3.5 Authentication and Access 16
6.4 Licence Database 16
6.5 Firmware Loading 17
6.6 Command Centre Hardening Guide 17
6.7 Gallagher's guide to security levels document 17
6.8 Gallagher Command Centre Cryptography and Encryption Technical Information Paper (TIP) 17

Copyright © Gallagher Group Limited

7 Flaw Remediation Policy and Procedures 18
7.1 Issue Triage Process 18
7.2 Responding to Security Issues and Vulnerabilities 18
7.2.1 Responsible Disclosure 18
7.3 Communication to Channel and Customers 18
7.3.1 Major Version Releases 18
7.3.2 Maintenance Releases 19
7.3.3 Security Advisories 19

Copyright © Gallagher Group Limited

1 SDLC Software Development Lifecycle

1.1 SDLC Overview

Product Development for Gallagher Enterprise and High Security products is managed via a six-monthly feature release cycle.

The development teams follow an iterative (Agile) approach to design and deliver product features and enhancements. At a high level, our development process has several phases (Requirements, Design, Development, Testing, Automated Integration Test Authoring, Technical Documentation).

These phases are mapped to stages for tracking the work items in our workflow tracking tool (Azure DevOps) and visible in teams' Kanban processes.

There are quality controls built into the teams' workflow such as code reviews and automated testing.

Static Code analysis of Command Centre code is run on a nightly build, via SonarQube.

A mature suite of automated product integration tests is executed nightly. Each development team owns portions of these tests and are responsible for ensuring they pass and are reliable.

There are currently two dedicated Technical Writers in the Enterprise Security Solution Delivery team with responsibility to deliver suitable technical documentation for Command Centre users, our technical staff and Channel Partners. This documentation includes installation notes for hardware and software, a server security hardening guide, release notes, user guides, in-system help documentation etc.

Each major release of our Enterprise product culminates in:

- a penetration test of the product conducted by an independent security penetration testing firm. A high-level penetration test history is available on request.
- a Beta test of the new software by first applying it on Gallagher buildings worldwide (internal Beta), followed by a managed Insider Program on several selected customer sites – see 5.5.

Each Command Centre release is accompanied by a Feature Summary, a Release Note that specifies the version number and the installation and upgrade procedures, and a Hardening Guide that explains how to take advantage of the security improvements in the new version. Some instructions are only applicable to certain customers based on their existing configuration.

Related internal documents:

- *High-Level Software Development Process*
- *Azure DevOps Work Item Guidelines*

Maintenance Releases (MRs) are also released between each major release version, these contain fixes and minor enhancements related to site issues or security advisories.

A *Release History* document is created for each Maintenance Release, which gives detail on these fixes and enhancements. It is distributed with the relevant MR software.

1.2 Physical Security

Gallagher's Command Centre security product is installed on our Hamilton New Zealand HO site.

Visitors to areas including R&D activity must be escorted by approved Gallagher personnel.

After-hours access to the buildings containing R&D areas requires dual factor authentication.

Copyright © Gallagher Group Limited

Access to the High Security room is restricted to personnel with NZ Government clearance only, unless escorted by an approved person.

Regular physical security site reviews are performed by the Security Risk Coordinator, in collaboration with the internal penetration testing team. Treatment and escalation of any identified risks is managed by the Security Risk Coordinator. These are logged and tracked within an internal Physical Risk Register. This register is maintained and reported on within the Risk and Responsibility team.

1.3 Employee Security

1.3.1 Hiring Process

As part of the new personnel hiring process, all potential hires undergo both drug testing and personality testing through trusted partners, as well as criminal history checks by the NZ Police A minimum of 2 references are required for all new hires.

Adherence to Gallagher's policy for handling of Security & Confidential Information is a standard condition of employment. All new staff undergo a corporate induction, which includes mandatory Privacy awareness training.

Personnel working in the High Security area require a minimum of Confidential level clearance from the NZ Government. These clearances, for each High Security team member, must be reviewed and reissued every 5 years.

Gallagher's Security Risk Coordinator supports our internal staff hiring and security training processes. This role is aligned to the NZ government's Protective Security Requirements (PSR) – a security framework covering Physical security, Personnel security, Information security, and Security Governance.

1.3.2 Training Material – Security Awareness

Several security related courses exist on our internal online training platform (Litmos). These are intended to introduce new team members to relevant security concepts:

- Information Security Awareness
- Introduction to Gallagher Intellectual Property Protection
- Privacy Awareness
- R&D Security Introduction

1.4 Procedural Security

1.4.1 Access to Security Issues and Vulnerabilities

Identified product security issues are managed in a Security backlog in Azure DevOps. Access to the Security Backlog is limited to specific R&D, senior Risk and Product Management staff.

See 7.2 Responding to Security Issues and Vulnerabilities

1.4.2 Responsible Disclosure

See *https://security.gallagher.com/en/Responsible-Disclosure-Policy*

Copyright © Gallagher Group Limited

1.4.3 Password security

Gallagher has an agreed standard for password security that follows NIST guidelines.

MFA is applied and enforced across all Gallagher accounts via the Microsoft Authenticator App or SMS verification. Client certificates are also assigned to Gallagher staff which are used to strengthen the authentication process.

Related internal document: *2.24 Password Mandatory Standard*

1.4.4 Code Review and Check in Policy

The code review and check in policy is defined in this internal document: *Code Review Policy.pdf*

For Git code repositories, changes to production code require a pull request which must be code reviewed and approved by a minimum of one other developer.

1.4.5 Release Branch Management Strategy

At a high level, our branch management approach is founded on a long-lived branch for development and long-lived release branches for each candidate release.

Short-lived feature branches are only created if it is believed the initial feature development could risk instability of the main branch for a significant period. These feature branches are merged in as soon as the risk has been averted.

Developer access to release branches is strictly controlled. When changes are required to a release branch the developer must submit a Pull Request, which enforces a code review from a team of "gatekeeper" developers.

Related internal documents:

- *Command Centre Code Branch Management Approach*
- *Command Centre Mobile App Release branch process*

1.5 Quality Management System

The Gallagher factory is certified to ISO9001. It includes a dedicated Quality team.

Related internal documents:

- *Quality Management System*
- *Appendix 1 – List of Interested Parties, Legal and Other Requirements*
- *Appendix 3 – Roles and Responsibilities*
- *Appendix 4 – Internal Audit Plan*
- *Appendix 5 – Process Change Management*
- *Appendix 6 – Calibration of test equipment*
- *Appendix 7 – Control of Non-conforming product*
- *Appendix 8 – Control of Documents and Records*
- *Appendix 9 – Product Concession*
- *Appendix 10 – Internal Audit Plan*

Copyright © Gallagher Group Limited

1.6 Information Security Management System (ISMS)

Gallagher's ISMS structure exists to support and improve the Information Security posture of Gallagher. This includes reviewing existing Information Security risks, planning, and orchestrating treatment for any risks outside of appetite, evaluating the effectiveness of those treatments, and continually improving the processes and controls in place that seek to address those risks.

The ISMS itself is scoped to consider, treat, and evaluate information security risks arising:

- at all Gallagher offices globally, and any site where Gallagher information is stored or processed; and,
- within all organisational business units, with appropriate representation from within those units; and,
- across all Gallagher Information Systems, including cloud or on-prem infrastructure, desktop or mobile computing devices, all forms of portable media, and any data processors engaged by Gallagher; and,
- within server rooms, network wiring, cloud services, videoconferencing platforms, and phone systems; and,
- from any external service providers including Software-, Infrastructure-, or Platform-as-a-Service providers; contractors, HVAC and Building Management systems providers, internet providers, electrical supply, etc.

Gallagher has and maintains ISO27001[1] certification for "*Professional engineering services, sales order management, and technical support, pertaining to Gallagher Security products - as delivered from Gallagher Global Headquarters, 181 Kahikatea Drive, Hamilton, New Zealand.*" [2]

An ISMS Governance Group consists of the Executive leadership team and meet regularly to review and manage information risks and controls for the business, while a ISMS Steering Group is responsible for implementation and reporting of any applicable processes and certification.

Gallagher has and maintains SOC2 Type II for "*Command Centre Cloud Hosted Services*"

1.7 Business Continuity Management

All critical R&D and Gallagher IS infrastructure is covered by a 24x7, 4-hour onsite service level agreement. with IS staff and warranty providers being on call outside of normal business hours.

If a service or system is not functioning or available, R&D log a request with IS for the fault, priority is assigned based on the service impacted.

Related internal document: *RnD Disaster Recovery Overview*

1.8 Disaster Recovery Policy

The following internal documents describe Gallagher's Backup and Restore Processes:

- *Gallagher Backup Process for RD related systems.docx*
- *Backup Restore flow chart.pdf*

[1] ISO/IEC 27001:2013 standard

Copyright © Gallagher Group Limited

2 Secure Coding Standard

Related internal documents:

- *Secure Coding Standard*
- *CCFT C++ Coding Conventions*
- *CCFT C# Coding Conventions*
- *Embedded C, EC++ and Assembler Coding Convention*
- *Test Automation Guideline*

Copyright © Gallagher Group Limited

3 Configuration Management System (CMS)

3.1 Source Control

Application source code is hosted in Azure DevOps Server or GitHub.com in a combination of TFVC (Team Foundation Version Control) and Git repositories. Pre-packaged build dependencies (most commonly third-party libraries) are hosted in our artifact repository (Artifactory).

Access to source code is restricted to Gallagher domain accounts that are also members of an appropriate Active Directory or Azure DevOps group which control read & write access to one or more repositories. Access to release branches is further restricted based on additional groups & Azure DevOps branch policy or GitHub Rulesets.A branch is created in source control for each major product release to support ongoing maintenance of that release (e.g. bug fixes).

For production code repositories in TFVC, a check-in policy encourages each commit to be associated with an Azure DevOps work item. In the unlikely event where a work item is not referenced in a code commit, Azure DevOps sends a notification to a senior developer.

For production code repositories in Git there are technical constraints that require a work item to be associated with each commit as well as requiring code review approval.

3.2 Builds

Product builds are automated using Azure DevOps Server's build system or GitHub workflows. Each build is assigned a unique version number by the build system and linked to a specific source control revision. Build scripts are version controlled and stored in Azure DevOps Server or on GitHub.com.

3.3 Build Machines

Access to build machines is restricted and changes to the build machine configurations are recorded on a wiki page. Builds for currently supported Command Centre releases are container-based, with the container build scripts maintained in source control.

Operating system updates are managed by Gallagher's Information Services department using Windows Server Update Services (WSUS) for Windows build machines. Linux build machines are configured to automatically apply operating system updates on a schedule.

3.4 Work Items

Work items (e.g. bug/feature tickets) are managed in Azure DevOps Server. Each change to a work item is audited and the work item is linked to related check-ins. Our check-in policy requires each check-in to be associated with a work item.

3.5 ECN (Engineering Change Notice) process

Ensures all changes to production systems go through a rigorous approval process and provides checklists that must be signed off for each change. This includes changing the version of firmware that is to be loaded during production. Related internal document: *ECN Process*

Copyright © Gallagher Group Limited

4 Security Policy / Processes/ Procedures

4.1 Security Related Company Policies

Defined in the following internal security related policy documents:

- *1.11 Security and Confidential Information Policy*
- *2.21 Information Security Policy*
- *2.23 Social Media Policy*
- *2.24 Password Mandatory Standard*
- *2.25 Logging and Monitoring Policy*
- *2.26 Information Security Guidelines for Users*
- *2.27 Website Security Policy*
- *2.28 Information Classification Policy*

4.2 Security Related Processes

4.2.1 Threat Modelling Process

In the context of software development at Gallagher, threat modelling is the identification of potential security vulnerabilities in a software system along with the mitigations that address those vulnerabilities. This is specified in this internal document: *Threat Modelling Process*

4.2.2 Security Design Reviews

We have a questionnaire in the development workflow to assess whether a security design review or threat modelling is appropriate for a given feature. This step is included in this internal document: *Enterprise Security Definition of Done*.

Related internal document: *Security Review Questionnaire*

4.2.3 Independent Penetration Testing

We engage a third-party company to conduct security code reviews and penetration testing for each major release (see 5.1.4). High risk developments may have additional testing done out of band to this. We have a letter that is produced for customers by the company we use for this testing that gives a high-level overview of what has been tested in each version.

We also engage with other security researchers, providing equipment, software and licensing for their research projects and maintaining good relations so that any items discovered are reported to us for fixing before being made public.

4.2.4 Approach for Managing Specific Site Data

Sometimes access to site-specific data can enable Gallagher to diagnose and address issues customers are experiencing with Command Centre.

Our approach to handling of site-specific data is outlined in this document: *Gallagher Security – Site Data Policy*. Key elements of our approach include:

- Customers are encouraged to run a data anonymisation utility on the database copy they send to us prior to sending. The utility either removes sensitive data (e.g. passwords) or replaces site-specific data names with generic terms, thus protecting sensitive or personal data from any risk of misuse.
- Site Data will only be used for the purpose for which it was collected.

Copyright © Gallagher Group Limited

- All Site data is held in a secure location on Gallagher Group's internal network. Access to this location is only allocated to certain Gallagher staff on approval from the Technical Support Manager
- Where possible, all data should be pre-encrypted on-site using AES-256 with a strong password or complex passphrase.
- Data collected can only be used for the purpose it was collected
- Unless specifically agreed, data is disposed of within six months.

Copyright © Gallagher Group Limited

5 High Level Testing and Verification Approach

5.1 Alpha Testing Process

All software developed passes through several testing processes:

- Developers implement unit tests and make use of the automation framework to test where appropriate
- Code is handed over to testers and they design testcases based on requirements and developer design documentation (using Azure dev ops work items)
- Testcases are reviewed within the team
- Alpha testing is completed, bug work items raised for failures and fixes implemented accordingly
- Automated tests are written and reviewed and checked into the automation framework and monitored for failures.

Related internal documents:

- *High level testing activities*
- *Planning and writing testcases*

5.2 Automated Testing Process

Gallagher has a team that is responsible for maintaining our automated integration test framework and platform that runs nightly integration tests.

- Automation of all the tests currently checked in is run every night on the development branch and (at least) the previously released branch.
- Each automated test is allocated to a specific team to monitor, maintain & ensure failures are rectified.
- The nightly automation runs are used as a go/no go for release of software from R&D into beta/full Release

Related internal document: *Automation Documentation*

5.3 Independent penetration testing

Items are evaluated by teams based on the threat modelling process. We do internal penetration testing where required to confirm issues or gain additional assurance for a new feature. For each major release there is a white box third party penetration test against new or changed features that have been identified as critical or high risk from internal reviews. The latest 'Security Assessment Statement Letter' signed by the third party is available on request.

5.4 Software Release Process

As mentioned previously, our release process for major Command Centre versions follows several phases.

Initially the new software is installed on Gallagher buildings worldwide. Our Solutions Engineering and Release Management teams complete a user acceptance test in multiple environments which includes a Digital Twin environment and our production system.

Digital Twin is a virtual server environment which simulates a real customer site specification. It includes the server operating system, SQL databases and computing resources.

Copyright © Gallagher Group Limited

The second step is to deploy the software on a limited number of Insider program sites to ensure that the product works across different server environments and network configurations.

Once the team are satisfied that the software is working as intended and in agreement with the Security Business Unit, software is full released and made available to all customers.

Throughout these phases, several builds of the software are deployed with incremental improvements. Each of these pre-release builds includes:

- Release documentation with a link to enhancements and bug fix work items implemented
- A hashed version of the software media available for download (or provided on USB)

Any defects found are raised as bug work items and triaged daily. Depending upon the assessed severity / priority of the identified defect, they are resolved in the next incremental build and re-deployed.

Related internal documents:

- *Command Centre Release*
- *Controller Release Process*
- *ECN process*
- *Full Release process*
- *Mobile Client Release*
- *Software Control Documentation Database*

5.5 Insider Program

During the Insider program process, pre-release software or the potential release candidate is deployed on selected Insider sites. These sites are directly supported by our team of Gallagher technical representatives and engineers to test the reliability of the product and its features. If any high or critical priority issues are identified on Insider sites, they will be investigated and fixed before the software prior to full release. Related internal document: *Beta Release Process*

Copyright © Gallagher Group Limited

6 Secure Delivery Procedures

6.1 3rd Party software

Artifactory is used as a repository for third party software components that are incorporated into Command Centre, where the component is unsuitable to store within source control.

Packages within Artifactory are either cached from the official package repository, or outputs from a Gallagher build machine.

Third party components used by Command Centre are tracked and there is a documented process for developers when considering adding additional components to Command Centre.

The software packages are then incorporated into Command Centre builds, which are subsequently tested, beta released, and formally released when the build has passed all levels of QA.

6.2 Gallagher Supplied software

Command Centre is built and signed on dedicated build machines, with the output placed on a shared drive which has restricted access. The in-file signature is a Microsoft Authenticode SHA256 digest, signed by a CA issued code signing certificate.

The Hardening Guide that is shipped with the product also details instructions for customers to generate and verify digests (hashes) of the executable files supplied.

6.3 Command Centre Cloud Infrastructure

6.3.1 Functional overview

Command Centre Cloud is a component of the system, which provides supporting services for Gallagher's Mobile Applications (Mobile Connect and Command Centre Mobile).

In the future, Gallagher intends to extend and introduce new cloud-based services in Command Centre Cloud in response to our customers' requirements.

6.3.2 Data transmission

Data transfer between Command Centre, the Cloud and Mobile devices uses encrypted HTTPS.
Gallagher supports only TLS 1.2; Older protocols are disallowed which mitigates most encryption-related security risks. You can view the SSL Labs industry standard report here:

https://www.ssllabs.com/ssltest/analyze.html?d=commandcentre%2dap%2dsoutheast%2d2.security.gallagher.cloud&latest

Communication between Command Centre and the Cloud servers is authenticated using TLS client certificates (2048-bit RSA).

Communication between Mobile devices and the Gallagher Cloud is authenticated using FIDO (P256 Elliptic Curve).

Copyright © Gallagher Group Limited

6.3.3 Cloud Services

Command Centre cloud is securely hosted using Amazon Web Services in Sydney, Australia. It is isolated from other Gallagher or external services using an AWS Virtual Private Cloud.

The cloud services themselves are not exposed directly to the internet, all traffic is routed through a dedicated Security Gateway component, which employs OWASP standard rules and techniques for mitigating attacks, as well as application-specific URL allow-listing and appropriate rate limiting.

Strict firewall and access control rules are in place protecting all Administrative functions and other endpoints.

All administrative users accessing our cloud infrastructure require two-factor authentication and strong passwords.

Services within the cloud environment are only allowed access to the minimum set of resources they require to function (e.g. they are only allowed to fetch and connect to the sole database / key storage they require and cannot access resources for any other services).

6.3.4 Command Centre Cloud Data storage and Approach

Command Centre Cloud contains:

- Data for the Mobile Connect app as defined in *Mobile Connect Cloud and App Security Technical Information Paper*
- Push notifications for Alarms for the Command Centre mobile app, as per the *Command Centre Mobile App Security Technical Information Paper*
- Only authorized DevOps administrators have access to mobile related data, and only for a specific purpose such as resolving a problem.

6.3.5 Authentication and Access

AWS IAM (integrated access management) with multi-factor authentication. DevOps team subject to security vetting process.

Gallagher staff authenticate with Azure Active Directory/Office365 when accessing CEIP data, also with multi-factor authentication.

Related documents:

- *Mobile Connect Cloud and App Security Technical Information Paper*
- *Mobile End to End Encryption*
- *Command Centre Mobile App Security Technical Information Paper*

6.4 Licence Database

Gallagher Security Software is controlled using a licence file. Each site is allocated a unique licence file "CommandCentre.lic" which is loaded onto the site's server, this enables functionality and enforces version control and proper use via the nomination of hardware (key device/s) located on the site (Controller MAC address).

Gallagher maintains a database of these licences. Gallagher access to the Licence database is inherited by AD Groups which are managed by the Information Services (IS) Team. Viewing the licence database is restricted to approved staff, however only Gallagher Security Technical Support and Sales Support teams are able to edit or generate full site licences.

Site licence changes can only be requested by the registered Channel Partner for the site, licences are emailed direct to a Channel Partner's company email address.

Copyright © Gallagher Group Limited

6.5 Firmware Loading

Firmware is built on dedicated Build Machines and output placed on a shared drive which limited people have access to. Edit access is limited to a few senior people.

To get this firmware into the factory it must go through an ECN process which ensures the appropriate people approve the change and fill out checklists to ensure everything is done correctly. The ECN process will result in the firmware being placed in a secure shared drive which factory workstations have read access to. Only limited people have the privileges to write to this location (see Official Folder Access doc).

TestStand modules are programmed to pull firmware from this location and load the firmware on to devices as part of the production process. Only Production Engineering staff have privileges to modify these automated processes.

Factory keys for controllers are only used to prove authenticity of the device during configuration. Keys to protect communications between Controllers, or between a Controller and its server are generated on site and pinned.

6.6 Command Centre Hardening Guide

This document contains information to help customers protect their Gallagher Command Centre systems from attack, increasing the overall security of their on-site installation. See *Gallagher Command Centre Hardening Guide*

6.7 Gallagher's guide to security levels document

This document contains information to help customers and Channel Partners analyse a site to determine its physical security level, and which Gallagher equipment and software is best suited to the site's requirements. It is intended for existing and potential Gallagher Security customers. See *Gallagher's guide to physical security levels*

6.8 Gallagher Command Centre Cryptography and Encryption Technical Information Paper (TIP)

This document, available on request, addresses questions regarding Gallagher Command Centre cryptography. It is intended to provide an overview of the encryption and authentication used by the Gallagher Command Centre Server, Controllers, and devices.

See *Gallagher Security Hub | Gallagher Command Centre Cryptography and Encryption TIP.pdf*

Copyright © Gallagher Group Limited

7 Flaw Remediation Policy and Procedures

As new features are developed, any functional and non-functional defects found must be addressed before that feature is considered complete, unless consciously accepted by the delivery team.

Software defects (bugs) are assessed for Severity and Priority according to agreed criteria.

Related internal document: *Azure DevOps Work Item Guidelines*

7.1 Issue Triage Process

Gallagher has dedicated Technical Support and Customer Response teams, focused on resolving problems raised by customers.

A cross-disciplinary Triage team with representatives from operations and R&D teams meet daily to assess the severity and priority of new customer issues and to route them to appropriate teams for resolution.

This overall process is mapped in Gallagher's internal *Issue Triage Process* document.

7.2 Responding to Security Issues and Vulnerabilities

Identified security issues are managed in a Security Backlog in Azure DevOps. Access to the Security Backlog is limited to specific senior staff within Solution Delivery.

The primary mechanism where new security vulnerabilities are triaged and prioritised are via regular meetings of the internal Cybersecurity Advisory & Triage group.

Product security incidents are constantly monitored using a combination of automated and manual techniques. We have an outreach programme for security researchers and actively engage with the hacker community to ensure we are aware of incidents as soon as possible.

When a serious incident is detected, an incident response team is formed to coordinate Gallagher's response.

The Cybersecurity Advisory & Triage group (CAT) is comprised of senior personnel and cyber security specialists. They determine the appropriate response and priority for security issues.

The overall process for responding to security issues is outlined in the internal document: *Dealing with Security Vulnerabilities*

7.2.1 Responsible Disclosure

See *https://security.gallagher.com/en/Responsible-Disclosure-Policy*

7.3 Communication to Channel and Customers

7.3.1 Major Version Releases

Major version releases of Command Centre are accompanied by a comprehensive marketing campaign (including feature summaries, fliers where appropriate, social posts, emails, promotional videos, website collateral, newsletter updates, updated existing marketing brochures etc).

Copyright © Gallagher Group Limited

7.3.2 Maintenance Releases

We publish regular maintenance releases for supported versions of Command Centre to resolve any defects impacting customers. Our Technical Support team publish regular Technical Bulletin newsletters to our Channel Partners.

7.3.3 Security Advisories

The Gallagher Marketing team manage the communication of relevant security issues.

We advise internal stakeholders of up-coming security advisories prior to maintenance releases being published. When the maintenance releases are published, we advise Channel Partners and customers who opt in via either the Customer Experience Improvement Program, or the Insider Program.

Two weeks after we advise Channel Partners and customers. We publish Security Advisories on our website (https://security.gallagher.com/en/Security-Advisories). The two-week delay is to allow sites to upgrade prior to any vulnerabilities being publicly known.

We are a registered CVE Naming Authority (CNA) who issue our own CVEs as per the MITRE framework. More details on this can be found at https://cve.mitre.org

Technical Support also post these advisories to our Support site for Channel Partners.

Related internal document: *Marketing Process – Security Advisories*

Copyright © Gallagher Group Limited