Service Definition Document

Service Model

SFG20

The Service

The Building Engineering Services Association (BESA) Group introduced the SFG20 standard in 1990 to ensure consistent and compliant building maintenance. The standard is constantly updated by our team of SFG20 technical authors.

SFG20 Service Model provides access to SFG20 maintenance schedules and supporting updates, with integration options for customers operating their own CAFM or operating software solutions.

Service Model Features

Library of over 1,500 maintenance schedules, colour coded by criticality.

Dynamic content updates aligning with changing UK legislation.

Regular SFG20 technical bulletin emails, providing updates regarding upcoming legislative, regulatory, and content changes.

SFG20 schedules show tasks, frequencies, and skillsets based upon regulations and user input.

Connectivity with customer operating software solutions via our bespoke SFG20 API.

Upon subscription, customers are provided with the necessary API documentation, ensuring a comprehensive understanding of accessibility, functionality, and integration capability.

Customers can utilise SFG20's internal API test environment (OTE) for compatibility testing.

Service Model Benefits

- Clear visibility of statutory and optimal maintenance.
- Avoidance of over and under maintenance.
- Continued compliance and prior knowledge regarding sector changes.
- Reduced maintenance costs and streamlined processes.
- Bespoke, structured planning and resource optimisation.
- Eliminate integration errors resulting from manual data uploads.
- Tender processes can be streamlined by specifying custom requirements to contractors using SFG20 schedules.

Customisation

The SFG20 system incorporates extensive customisable functionality, maximising accessibility, capability, and individuality. Provided that users have an access level above read only, they can create their own unique custom schedules, incorporating bespoke elements which can be influenced by the user, such as:

- Technical content.
- Task frequencies.
- Skill set requirements.

These aspects can be added, amended, or removed within custom schedules dependent upon customer preference. Additionally, criticality ratings can also be assigned depending on the product subscription. There are four criticality ratings that customers can allocate across schedules, which include:

Statutory
Must be completed, ensuring asset alignment with statutory regulation.

Business Critical
Must be completed for safe continuity of service.

Optimal
Should be completed for maximum asset efficiency and high-quality service.

Discretionary
Can be completed at the customer's discretion.

Acting in accordance with ISO 22301, BESA Group operate robust business continuity, disaster recovery, and contingency measures, engaging the optimum assessment and systematic response methods, minimising disruption caused by an emergency.

Continuity plans and procedures are reviewed annually, or whenever lessons learnt must be implemented, by Head of Operations, with oversight from our Chief Technology Officer. Our recovery plans have four objectives:

Define and prioritise the critical functions of the business

Analyse the emergency risks to the business

Detail the agreed response to an emergency

Identify key contacts during an emergency

When delivering service, we understand that continuous and developing threats can be posed and, as such, we have developed bespoke service-specific assessments, identifying primary risks that could hinder service delivery and outlining our procedures for mitigating their impact. By doing so, we proactively ensure business and service continuity, whether these hazards come into effect or otherwise. Through a combination of likelihood and adverse impact upon service, BESA Group recognise and mitigate potential disruptions.

To ensure that disaster recovery remains compliant with standards and addresses the most contemporary risks, we commit bi-annual disaster recovery tests, identifying efficacy, potential improvement, and developing risks. Our continuity assessments and disaster recovery plans include contingency for the following events:

- Illness outbreaks and widespread unexpected absenteeism.
- Physical disasters and premises damage.
- Data loss and cyber-attacks.
- Power outages.
- Supply chain shortfalls.

Our business continuity plan (BCP) is updated for each customer and is integrated into our management processes as standard. The BCP is audited annually with a report being made available to our customers on completion.

Onboarding and Offloading Support

BESA Group deliver a comprehensive onboarding support service upon subscription with our platform, SFG20 Service Model, including training and demonstrations, which incorporate a free online demonstration service before purchase. Our onboarding procedures are delivered by system experts, ensuring that users develop a comprehensive, accessible understanding of system functionality. Regular technical bulletin emails advise subscribers of upcoming changes in regulation and new and updated SFG20 content.

Customers have the opportunity to enrol in instructor-led onboarding training sessions conducted by our expert trainers. (additional fees apply).

Service Model training includes the following:

- Create an asset profile to demonstrate compliance to stakeholders.
- Build a bespoke maintenance plan, to facilitate efficient team working and streamline tender processes.
- Download data – for use with CAFM systems and maintenance teams.
- Customise specialist schedules to individual requirements.

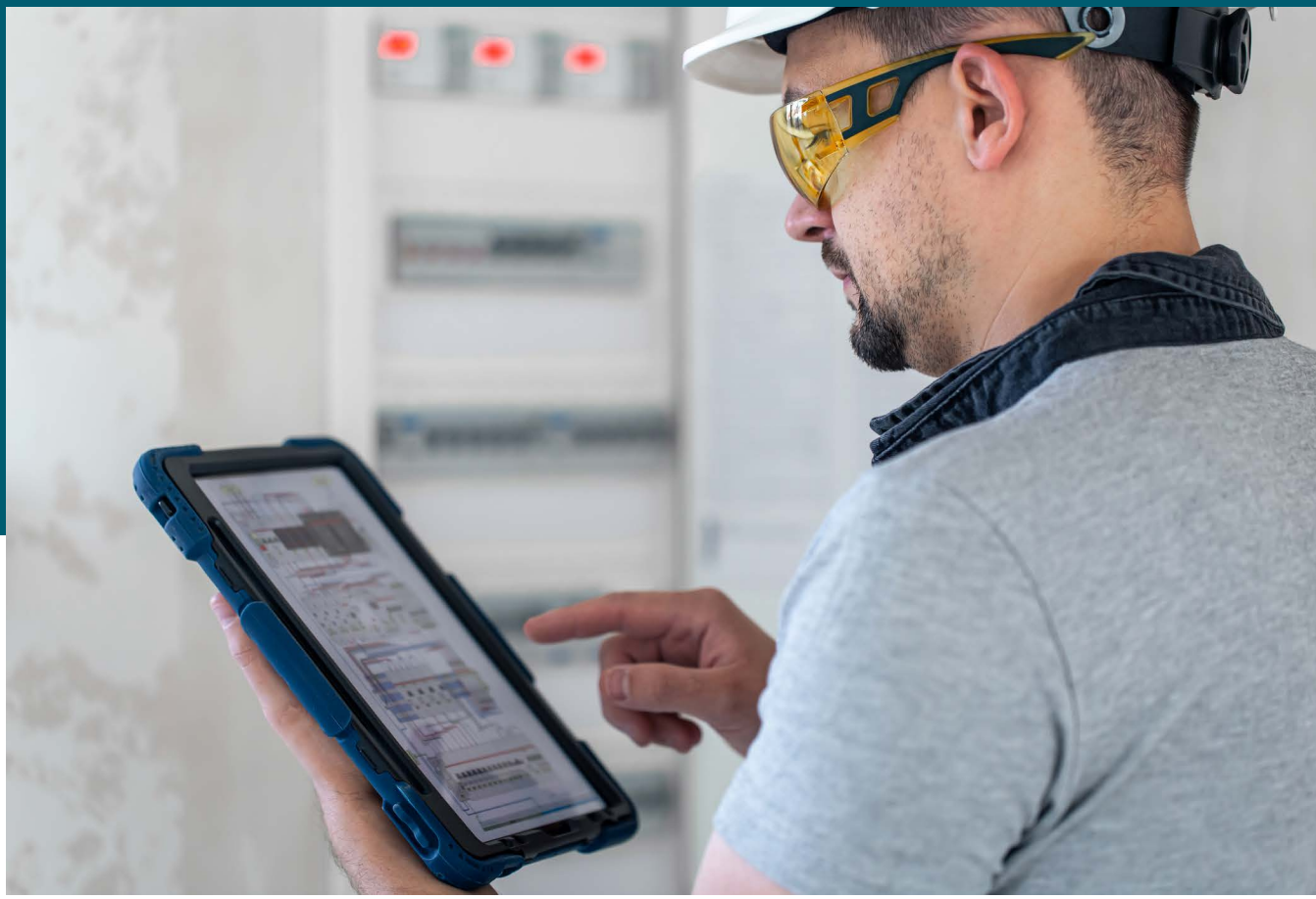
The objective is to equip customers with a comprehensive understanding of the software solution and enable them to practically apply their knowledge, using a case study.

Upon cancellation of subscription, the customer will lose access to functionality upon completion of payment period, and access to the SFG20 Service Model system and content will be revoked. As our content is dynamically updated based upon legislative changes, content held by the customer would not be contemporary, compliant, or usable beyond the latest updates. When cancelling a non-contractual license, there is no additional cost to the customer, nor when reactivating the license during the future. However, when under a contracted license, the customer will have to pay up until the termination date.

Service Constraints

Service Model is a SaaS and requires users to have suitable connectivity and supported devices/ browsers. However, extra constraints may be implemented during periods of maintenance, update, or reconfiguration, which will always be brought to user attention before commencement. Additionally, the service is protected by requiring users to access their official registered email address, securing the system and imposing constraints on unauthorised access.

All our methods are defined following industry best practice and are integrated into our management processes as standard and are audited annually with a report being made available to our customers on completion.



Service Levels
(Performance, Availability and Support Hours)

The support levels provided by Service Model are comprehensive and accommodate the requirements of users throughout service delivery.

Service Management

Availability

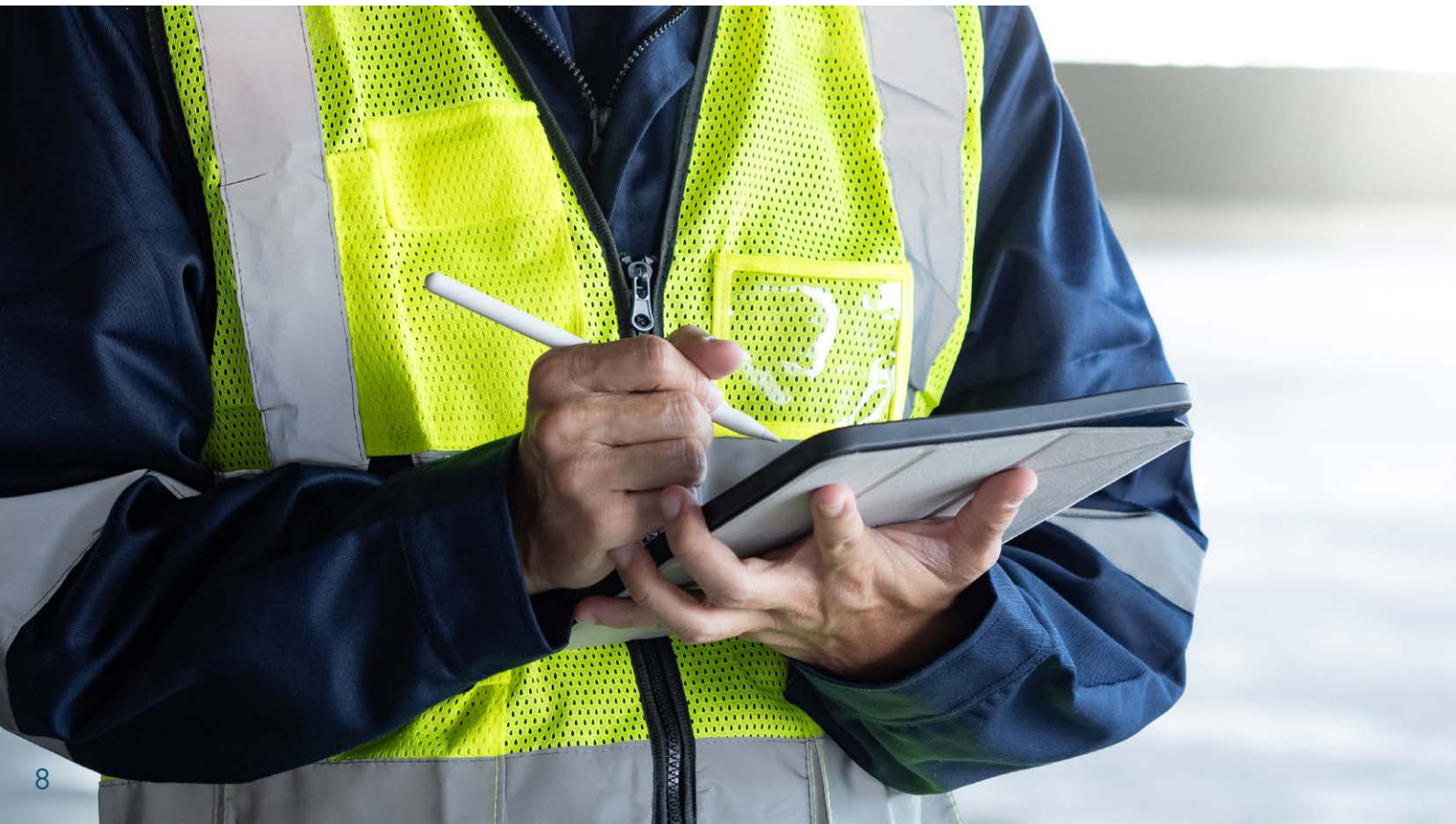
Availability is expressed as a service-level target to support buyer evaluation. Where a call-off contract specifies different terms, the call-off terms take precedence. Availability target: 99.9% monthly availability for the Service Model service, excluding planned maintenance windows.

Planned maintenance

Planned maintenance is scheduled to minimise disruption and is normally performed outside standard support hours. Advance notice is provided to customers where practical.

Incident management

Incidents are prioritised based on impact and urgency. First-response targets are provided below. Resolution times depend on root cause and may require workarounds, fixes or planned releases.



After Sales Support

BESA Group have a dedicated help desk which supports utilisation of the SFG20 system post-sale, which is facilitated by system experts and developers, delivering case-specific, continuous, and dedicated support. Queries regarding BESA Group products should be communicated via the following methodologies, which can be accessed between 9:00am-5:00pm:

Email:
info@SFG20.co.uk

Post:
Old Mansion House, Eamont Bridge, Penrith, Cumbria, CA10 2BX, UK

Phone:
01768 860 459

Contact Us Form:
www.sfg20.co.uk/contact

Customers are likely to receive prompt service via telecommunication and email provided that the information relayed pertains to the issue and accurately delivers an understanding of the problem.

Overall charges for subscription to the SFG20 service cover support inclusion, ensuring that system discrepancies can be rectified, except for on-site support, which may incur additional charges. When updating the SFG20 systems, BESA Group will distribute bulletin updates, and information onto our website covering changes. Additionally, we can support third party engagement, provided they hold a SFG20 licence.

Technical Requirements

The system is supported by Chrome/Edge/Safari browsers and requires a minimum 8GB RAM and 1280x1024 minimum resolution.

Outage and Maintenance Management

Based upon the hosting environment's internal SLAs, should an outage occur, we will be notified by Microsoft Azure via email, push notifications, and our IT management tools. As we have 99.9% up time, we can provide rapid response regarding issues that impact customers, as our support team are readily available, communicating with customers directly via email.

A notification will be placed on our website, expressing the outage, and explaining the ongoing response; however, we understand that not every customer will access our website during this time and, therefore, may not become aware of the outage. As such, we will send continuous outage emails, updating on progress and expected service return. This ensures customers hold accessible information regarding an outage and can accommodate the downtime.

Once the outage has been resolved we then send a further email to customers notifying them and update our dashboard to notify anyone using our website that the outage has been resolved.

In the instance of faults where the system remains operational, but the function of some features are degraded, we will prioritise according to the following schedule:

Priority	Triage / 1st Response Time	Contact Frequency
Urgent	Within 1 hour	Daily
High	Within 3 hour	Daily
Medium	Within 1 day	Weekly / Monthly as agreed per incident
Low	Within 2 days	On changes of status / work carried out

Priority Key:

Urgent: Service is unavailable, or there is a significant loss of core functionality affecting many users.
E.g. Login outage; Regime/schedule access unavailable.

High: Severe degradation or a critical feature is unavailable with a limited workaround.
E.g. Key output failing; API connectivity interrupted.

Medium: Non-critical feature failure or limited impact with a workable alternative.
E.g. Minor output issue; intermittent UI defect.

Low: Minor issue, request, or cosmetic defect.
E.g. Text/UI formatting issue; minor usability request.

When managing software orders and invoices, SFG20 undergo the following process, ensuring compliance with statutory legislation and regulation:

- Discuss client requirements and system utility.
- Undergo quotation, with a sales contract emailed to the client for approval and signing.
- Receive signed contract from the client.
- Undertake account setup.
- Automated email sent to the client, notifying them of SFG20 solution login details.
- Client account set up within the financial system.
- Invoice created and sent to the client via email for payment – typically stipulating a thirty-day payment term.

We use appropriate tools and third party organisations to assess threats to our services. All change activity is managed, monitored, and tracked from initial development to production. This allows us to track the components of our services and monitor and report on any changes.

We are audited and certified against the Cyber Essentials Plus standard, so we can be confident that threats are getting dealt with accordingly and there are no vulnerability issues within our services. Our vulnerability management process is subject to yearly external review so we can ensure our process is effective and of a high quality.

Access to Data (Upon Exit)

Customers can terminate their subscription with our service whenever they feel it necessary, but they must pay until the end of their contract period. Conclusion of the subscription will remove the functionality of the system upon conclusion of the payment period and limit access to updated system outputs, including legislative changes, feature updates, and schedule management tools. We do not incorporate a cancellation fee but data which has not been exported before the payment period end date will be lost and cannot be recovered.

Data extraction via upload into the customer's CMMS system must be completed before the conclusion of the payment period, as data will not be recoverable beyond this timeframe. Furthermore, data extracted before termination will no longer receive update regarding legislation and regulation changes. However, terminated accounts are not permanently deleted and, therefore, customised data can be made recoverable upon reinstatement of a subscription.

Should a customer decide to terminate their contract, their licence will then be cancelled immediately, which will be confirmed via a cancellation email, with services ceasing at the end of their current payment period. Prior to the payment period closure, users will be prompted to remove any data, being reminded that the service will be unavailable moving forward. There are no associated costs to a user for cancelling their contract and, should they return to the service in the future, there are no extra costs associated with reacquisition. Should a client return after cancelling their contract, their new subscription would be costed at the current prevailing cost.

Security

In accordance with Cyber Essentials Plus, the Data Protection Act (2018) and GDPR policy, all personal data we hold is limited to the name, username, email address, record of account activities, transaction records, and subscriber organisation as applicable for each user. All personal data is processed only to the extent and for the duration necessary for the legitimate interest of performing our obligations under the contract with the subscriber by which a user is accessing our services. We are ICO registered and personal information is accessible to the appropriate individual upon request.

Additionally, we incorporate the following data protection procedures:

- We operate with secure VPN access for remote workers, ensuring security when off the main network.
- Data stored on computers/mobile phones are protected by passwords with two-step authentication and 'single sign-on'.
- We operate 'Next Generation' firewalls with linked endpoint anti-virus/anti-ransomware, keeping endpoints safe and the ability to block access to any compromised devices.
- All internal devices are required to have the latest security updates, ensuring that all hardware and software remains contemporary, minimising the possibility of data breaches.
- We engage with third party security specialists and the appropriate Cyber Insurance coverage, ensuring support in the event of suspected data breaches, as well as proactively mapping to ensure data security is maximised in the first place. Internally, cyber testing and security reviews are held annually, ensuring that our systems are resilient, secure, and compliant throughout the duration of usage.

Furthermore, information security and GDPR training is provided to employees, ensuring the principles of data security are reflected across service delivery, and system end users can be trained for data protection compliant and secure utilisation. The above procedures and overall information security systems are managed and overseen by the following individuals with appropriate responsibilities:

- Our Chief Technology Officer will ensure that integration and systems remain compliant with expectations, regulations, and legislation, including data protection, and maintains necessary resource. The systems and procedures are audited bi-annually, or whenever significant changes occur, implementing necessary information security training modules.
- Our team of GDPR officers cover subject access requests, GDPR employee advice and business support, and legal support, such as contracts management. The team oversee changes within data protection law and policies and manage data breach investigations.
- All employees receive GDPR training and are kept updated on company policy.
- Individual employees hold responsibility for maintaining the integrity and confidentiality of any assets provided by the company.

Should it be suspected that data protection protocols have been breached, we have implemented
contingency protocols which mitigate damage and secure the system, detailed as follows:

- Any potential breach will be reported to the Chief Technology Officer.
- Any potential breach will be subject to a data protection impact assessment (DPIA), which informs next steps, incident response, and associated communication plans regarding impacted stakeholders.
- All high-risk personnel will be informed of the breach.
- The DPIA is performed by Change Support Manager.
- Utilisation of the central back-up of client information.
- Utilisation of central back-up of employee information.

Any breach will be investigated and reported to the appropriate authority once the severity of breach has been determined. An incident response team will undertake an impact assessment of the incident, per GDPR requirements, determining individual risk, which will then inform next steps relating to GDPR, aligning with our data protection policy. If required, a team of business, IT and marketing stakeholders will then coordinate further activity.

SFG20

DRIVING FACILITIES EXCELLENCE

Contact your account manager or sales representative today to discuss how our services can benefit your organisation.

info@sfg20.co.uk 01768 860 459 sfg20.co.uk SFG20 @sfg20_