Village
Software Engineers

GCloud 12

Lot 2 - Cloud Software:

Supplier - Village Software Engineering Limited

Services Description:

Overview:

Village Software based out of Liverpool are a Microsoft GOLD, QPR Software and Tableau partner that specialises in application development, enterprise integration, process improvement, data management services, cloud deployment and busines intelligence solutions.

We have over the last 25 + years worked across many sectors providing innovative software solutions. Key markets include: Healthcare, Education, Government, Retail, Distribution, Manufacturing and Media.

We offer a full turn-key service that includes:

- Project Management
- Software tool selection
- Solution design
- Solution build and implementation
- Solution managed Services
- Cloud management, deployment and hosting
- Process improvement, mining and automation consultancy
- End user Training
- Named Account Management

We utilise the Agile project management methodology and typically work hand in glove with our client's own team. In most cases Village provide the "Scrum Master" and the project governance overlay.

As resellers of the Tableau, QPR and Microsoft technologies we offer a "Wrap around" service that ensures that our client gets true impartial advice and best practice deployment and implementation of the software toolsets. The breadth over our in-house skills, which include: Azure, AWS, Microsoft Power Platform, SSIS, SSAS, Azure data factory, Synapse, Databricks, Tableau, Python, R, Angular, C#, C++, SQLServer, Oracle, Java, Android and IOS, ensure we can offer a very innovative and modern solution from data integration and data warehousing to bespoke application development and sophisticated business analytics.

Our aim is to use software solutions to improve organisational performance and ensure our support services allow the client to self-manage their systems post go-live.

Pricing - fundamentals

Village Software typically contract with Public Authorities on a fixed price basis based on an outcome- based specification. Please also see our GCloud Prices document for further information.

We have also supplied an SFIA based rate card for GCloud 12 (please see separate document) and these rates cover our T&M based projects and individual consultancy engagements where a "pot of days" are purchased by the client. We do offer discounts for T&M based contracts based on the number of days used. These discounts will be agreed with individual clients and start at 20 + days.

We also offer day rate discounts for remote working, as opposed to on-site. We recommend for most projects that the majority of the input days are remotely delivered, this is to boost efficiency, save time and reduce expenses to as near to NIL as possible for the client. As an Azure specialist our remote working is all undertaken via and within Azure, to ensure maximum data security at all times.

Software is typically licenced on a SaaS basis and based around named users.

Invoicing

We generally invoice monthly in arrears for T&M based work, invoices are based on time input during the month x the agreed day rate. As most work is undertaken remotely we are happy to charge in 15 minute blocks. This offers great value to the client as they only pay for the actual time we are working on their project. For on-site work, we do not charge for travel time.

On fixed priced contracts we generally agree payment milestones based on delivery or a fixed payment profile. Milestones are detailed within the "Sprint Plan" and typically are:

- Contract signature
- Delivery of agreed workstream to UAT
- Workstream Sign off
- All Workstreams signed Off
- System Go-live

We agree each payment profile individually with each client.

SaaS invoicing is annually in advance

Data Protection and System Security Rider

1. **General.** This Data and Systems Security Rider (the "Security Rider") outlines particular administrative, logical, technical, and physical security requirements that Supplier shall maintain as part of, and to the extent applicable to, the Services and Deliverables ("Security Requirements"). These requirements are not intended to be exhaustive; Supplier shall at all times maintain an information security program (including formal written policies and procedures) sufficient to ensure the security and integrity of Customer Data and of the Supplier Systems, and to ensure compliance with applicable privacy and data security Laws and industry-accepted information security practices. The Security Requirements shall apply to all access to Customer Data, and all processing, storage, transmission, or maintenance of Customer Data and/or Customer Systems.

2. **Definitions; Conflict.** For purposes of this Security Rider, the definitions set forth in this Section shall apply. In the event of a conflict between the Security Rider and the Agreement, the Security Rider shall govern.
   a. **"Customer Data"** means any and all information, files, records, documentation, or other data collected, stored, accessed, processed, or transmitted by or on behalf of

Customer (or collected on or via Customer Systems), including but not limited to information relating to Customer, its Affiliates, consumers, customers, talent, partners, clients, personnel, employees, contractors, agents, and directors provided by Customer to Supplier. Customer Data includes, but is not limited to, Customer Personal Data.

b. **"Customer Personal Data"** means Customer Data that consists of any data that personally identifies, possibly could identify, or is reasonably linkable to an individual, and may include, but is not limited to: (a) name, address (e-mail or postal), telephone number, user ID, and passwords; (b) information such as a national identification number, passport number, social security number, or driver's license number; (c) financial information, such as a policy number, credit card number, and/or bank/financial account number; (d) sensitive personal data, such as mother's maiden name, race, marital status, health and medical information, gender, or sexuality; and/or (e) any other information that is deemed "personal information" or "personal data" under applicable Data Protection Laws.

c. **"Customer Systems"** means, collectively, the systems of Customer and its Affiliates, including computer systems, hardware, software, platforms, devices, equipment, websites, mobile sites, applications, and networks, and any other digital property or technology owned, controlled, or operated by Customer and/or any of its Affiliates.

d. **"Data Protection Law"** means any applicable Law relating to data privacy or data protection and guidance, directions, determinations, codes of practice, circulars, orders, notices, or demands issued by any competent data protection authority.

e. **"Deliverables"** means the deliverables described in the Agreement or any attachment thereto.

f. **"Law"** means any national, provincial, state, or local statute, law, ordinance, directive, regulation, rule, code, order, or other requirement or rule of law, including the common law, of any country, region, or governmental body.

g. **"Maintenance Tools"** are tools used for diagnostic and repair actions on organizational information systems and include hardware, software, firmware items, diagnostic test equipment, and packet sniffers.

h. **"Malware"** means software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system, including, but not limited to, a virus, worm, Trojan horse, spyware, some forms of adware, and any other code-based entity that infects a host.

i. **"Removable Media"** is any type of storage device that can be removed from a computer while the system is running, including, but not limited to, portable devices that copy, save, store and/or move data rom on system to another such as: (a) any hardware that provides connectivity to USB devices through means such as wireless (WiFi, WiMAX, MiFi, irDA, Bluetooth, among others) or wired network access or mounted network shares; (b) removable memory based media (e.g., USB memory devices/readers, removable memory-based media (e.g., USB memory devices/readers, removable hard drives, flash drives, thumb drives, jump drives, key drives, rewritable DVDs, CDs, and floppy disks, magnetic tape reels, disk packs, floppy disks, and diskettes, disk cartridges, optical discs, paper tape, magnetic cards, memory chips, tape cassettes, FireWire devices, external serial advanced technology attachment devices and microcassettes); and (c) Memory cards (e.g., SD, CompactFlash, miniSD, microSD, and xD cards)

   a. which can be used to support a data storage function on digital cameras, PDAs and smart phones, MP3 and MPEG devices.

   b. **"Security Incident"** shall mean actual or suspected unauthorized access, acquisition, disclosure, or use of the Customer Data in Supplier's or Supplier Personnel's possession, custody, or control.

   c. **"Supplier Personnel"** shall include the officers, partners, employees, agents, and subcontractors of Supplier, Supplier's Affiliates, and Supplier's contractors and subcontractors.

   d. **"Supplier Systems"** means Supplier's networks, resources, platforms, devices, systems, servers, workstations, services, technology, and applications that access, process, transmit, or store Customer Data or access or connect to the Customer Systems.

e. **"Services"** means the services described in the Agreement or any attachment thereto.

3. **Access Management.**

a. Supplier shall access Customer Data and/or Customer Systems only in accordance with the Agreement or as otherwise instructed by Customer in writing. Customer reserves the right at any time to revoke Supplier's access to Customer Data and/or Customer Systems or to require Supplier to change the user IDs and passwords required for such access.

b. All access to the Customer Systems shall be via an Customer -approved secured connection between the Supplier Systems and Customer.

c. All Supplier Personnel connecting to the Customer Systems shall be identified by a unique token and user ID. Customer shall control the issuance of all tokens, and user IDs, and passwords for the Customer Systems. Access to the Supplier Systems and Customer Data located thereon shall require a user ID and password. The user ID shall enable the Supplier to complete an authentication procedure in relation either to a specific processing operation or to a set of processing operations. Passwords for the Supplier Systems used for processing Customer Data and/or accessing the Customer Systems shall be (a) changed at least once every ninety days; (b) consist of at least ten characters, including small and capital letters, numbers and special characters; (c) shall not contain any item that can be easily related to the person in charge of the processing; and (d) shall be at least one day old before change is permitted, and the previous ten passwords shall not be reused. After a maximum of ten consecutive failed login attempts, system access for the account shall be disabled for a period of at least thirty minutes.

d. Passwords for access to Customer Data and/or Customer Systems shall be stored securely, not in plain text, on a separate server or file from Customer Data, and not labeled in folders that are easy for hackers to find (e.g., folders labeled "passwords"). Supplier shall not share access credentials with third parties. Where the Supplier processes non-US Customer Personal Data, in addition to the above, the user IDS shall be deactivated if they have not been used for six (6) months or more, except for those that have been authorized exclusively for technical management purposes.

4. **Supplier Personnel.**

a. Only Supplier Personnel that have a need to access Customer Data and/or Customer Systems to provide the Services will have the ability to do so, and only to the extent necessary to perform such Services. When any Supplier Personnel no longer has a business need for the access privileges to Customer Data and/or Customer Systems assigned to him/her, the access privileges shall be promptly revoked, even if such Supplier Personnel continues to be an employee, agent, or contractor of Supplier. Supplier shall not permit any Supplier Personnel, contractor, or third party other than those authorized by Customer pursuant to the Agreement to access the Customer Data and/or Customer Systems. Where the Supplier processes non-US Customer Personal Data, in addition to the above, the Supplier shall regularly verify, on at least an annual basis, that the Supplier Personnel continue to have a need to access Customer Data and/or Customer Systems to provide the Services.

b. Supplier shall maintain policies that require its Supplier Personnel to report suspected violations of the confidentiality terms of the Agreement, the Security Requirements, and suspected violations of Supplier's data security policies to Supplier management for investigation and action.

c. Supplier must ensure that all Supplier Personnel who access Customer Data and/or Customer Systems: (i) attend confidentiality and security awareness training at least once per year; (ii) are fully informed (at least annually) of, and monitored for adherence to, the Security Requirements and Supplier's data security policies and standards, and (iii) are subject to disciplinary action (and/or legal action where appropriate) for violations of same.

d. Except as provided herein, Supplier, or its agent, shall perform a local, state, and federal background investigation ("Background Investigation") on all Supplier Personnel performing Services under the Agreement or otherwise having access to Customer Data. Supplier shall contractually obligate all subcontractors performing Services to perform such Background Investigation on any subcontractor personnel performing Services under the Agreement. The Background Investigation shall include a detailed examination of (i) criminal convictions involving a dishonest act (including but not limited to fraud, theft, and embezzlement), and (ii) injury or threatened injury to another person. Supplier shall not permit any Supplier Personnel or subcontractor personnel with a criminal record falling into categories (i) and (ii) above to perform Services under this Agreement or gain access to Customer Data and/or Customer Systems. Supplier shall not conduct the Background Check where such check is prohibited by applicable Law, and shall instead provide notice of same to Customer. In such case, Supplier and Customer will agree on the appropriate level of background check before any such Service Provider Personnel perform Services.

e. Supplier shall ensure immediate revocation or deletion of all access rights to Customer Data and/or Customer Systems for any terminated, leave of absence, or transferred Supplier Personnel, and notify Customer of the same. Supplier shall obligate Supplier Personnel to return or destroy (as directed by Customer) any Customer Data within Supplier Personnel's possession within 48 hours of termination, leave of absence, or transfer, and Supplier shall confirm and notify Customer of the same.

f. Customer Data may not be stored or accessed by Supplier Personnel on personal accounts (e.g., individual email or cloud services accounts) or stored locally on personally-owned computers, devices, or media. With respect to its own Personnel, Supplier shall implement technical controls to prevent downloading of Customer Data onto personally-owned computers, devices, or media.

5. **Physical Security Requirements.**

a. Customer Facilities. When present at an Customer facility, Supplier Personnel shall abide by all Customer security policies and any additional security requirements that have been provided by Customer to Supplier. Supplier must certify that those Supplier Personnel requiring unescorted access to Customer facilities have successfully completed a Background Investigation. Additionally, all Supplier Personnel located at an Customer facility must possess (and present upon request) photo identification in the form of a state/country provided document (i.e., Passport or driver's license). Supplier Personnel must wear an Customer-issued visitor ID badge while on Customer premises.

b. Supplier Facilities. Supplier must document and maintain, subject to Customer approval, adequate physical security controls and procedures over all Supplier facilities where Customer Data is received, processed, filed, or stored and where Customer Systems are accessed, including at a minimum, appropriate alarm systems, access controls (including off-hours controls), visitor access procedures, security guard force, fire suppression, environmental controls, video surveillance, and staff egress searches in a manner sufficient to prevent damage and unauthorized access to Customer Data and Customer Systems, and consistent with the below requirements:

i. Supplier must maintain physical barrier controls to prevent unauthorized entrance to Supplier facilities both at the perimeter and at building access points. Passage through the physical barriers at Supplier facilities shall require either electronic access control validation (e.g., card access systems, etc.) or validation by human security personnel (e.g., contract or in-house security guard service, receptionist, etc.). Supplier Personnel shall be assigned photo-ID badges that must be worn while such personnel are at any Supplier facilities. Visitors shall be required to sign-in with designated personnel, must show appropriate identification, shall be assigned a visitor ID badge that must be worn while the visitor is at any of Supplier facilities, and are continually escorted by authorized Supplier Personnel while visiting such facilities.

ii. All access points (other than main entry doors) shall be maintained in a secured (locked) state. Access points to Supplier facilities shall be monitored by video surveillance cameras designed to record all individuals accessing such facilities. Supplier shall maintain electronic intrusion detection systems designed to detect unauthorized access to the facilities, including monitoring points of vulnerability (e.g., primary entry doors, emergency egress doors, roof hatches, dock bay doors, etc.) with door contacts, glass breakage devices, interior motion-detection, or other devices designed to detect individuals attempting to gain access to Supplier facilities. All physical access to Supplier facilities by Supplier Personnel must be logged and routinely audited.

iii. Supplier shall securely store physical files, workstations, and devices that contain Customer Data and/or access Customer Systems in a manner sufficient to prevent unauthorized access to Customer Data and Customer Systems. Supplier shall maintain safety standards in place when Customer Data is en route, including training of Supplier Personnel regarding safe security practices and technical controls such as encryption of laptops, thumb drives, files, and disks to prevent access to Customer Data if the physical device or media is lost.

6. **System and Network Security.**

a. Supplier shall implement appropriate firewalls to manage and restrict network traffic, and shall properly segment its network, including establishment of a demilitarized zone (DMZ) for publicly-accessible servers. Where the Supplier processes non-US Customer Personal Data, in addition to the above, the Supplier shall carry out an update of the firewalls at least every six (6) months.

b. Supplier shall use an industry-accepted intrusion detection and prevention system to detect inappropriate, incorrect, or anomalous activity, and Supplier shall regularly monitor system logs for suspicious activity. Supplier shall allow Customer access to system security logs, latency statistics, etc. that affect Customer Data, and Supplier shall cooperate with Customer as requested in providing information and assistance relating to Customer Data processed through the Supplier Deliverables and Services (e.g., data corruption and restoration, access/activity logs). Supplier shall establish and follow operational procedures to stop or mitigate any real or reasonably foreseeable potential attack or attempted attack. Where the Supplier processes non-US Customer Personal Data, in addition to the above, the Supplier shall carry out an update of the industry-accepted intrusion detection and prevention systems at least every six (6) months.

c. Supplier must develop and maintain a written security incident response plan to guide Supplier Personnel in responding to a Security Incident and to ensure any such incidents are promptly addressed and remediated.

7. **Encryption.**

a. Supplier shall use encryption to secure Customer Data at all times at rest and in transit. Supplier's encryption shall be consistent with validated cryptography standards as specified in National Institute of Standards and Technology FIPS140-2, Security Requirements.

b. Supplier must use SSL with the highest encryption available when transferring Customer Data over the Internet.

c. Full disk or device encryption is required for all portable devices and removable media used by Supplier Personnel (e.g., laptops, flash drives, CD-ROMs, external hard drives, etc.) that store Customer Data.

8. **Backup, Business Continuity, and Disaster Recovery.** To the extent applicable to the Services to be performed, Supplier shall be responsible for developing and maintaining procedures for the backup of Customer Data and the recovery of destroyed, lost, or damaged Customer Data with respect to such data in the possession of Supplier or Supplier Personnel. Unless otherwise directed by Customer or specified in this Section, Supplier shall back up Customer Data on the last day of the month on a rolling one-hundred eighty (180) day cycle. At any time, Customer reserves the right to request a sealed, archived backup of Customer Data (reflecting a certain point in time as directed by Customer), and Supplier shall resume Services with such backup of Customer Data, as an available remediation action for a cryptolocker or ramsomware event. Supplier shall correct or recreate, to the extent possible, any destruction, loss, or damage of any Customer Data caused by Supplier or any Supplier Personnel or in the possession of or under the control of Supplier or Supplier Personnel using commercially reasonable efforts. Where the Supplier processes non-US Customer Personal Data, the following applies in addition to the above: (a) the Supplier Systems used for processing Customer Data shall be secured in particular against loss of Customer Data which may be caused by a failure of power supply or line interference; and (b) Supplier shall back up Customer Data on the last day of each week on a rolling one-hundred eighty (180) day cycle.

9. **Software.**

   a. If Supplier is providing software development services for Customer: (a) procedures must exist to physically and logically separate any application development and production servers and environments; and (b) live data, including direct copies of production Customer Data shall not be used in any non-production environment, including development and test systems.
   b. Supplier shall ensure that any software developed for, or licensed to, Customer in connection with the Agreement uses industry-standard secure coding practices.
   c. Supplier shall test for and remediate common vulnerabilities identified by the Open Web Application Security Project (OWASP) (e.g., Structured Query Language (SQL) injection attacks) in connection with developing, upgrading, or testing software for Customer, before delivering any software to Customer under the Agreement, and/or before using any software to perform Services for Customer. Supplier shall harden the software prior to delivery or use, ensuring only necessary ports and protocols are exposed, and/or provide a detailed configuration guide.
   d. In connection with any software developed for, or licensed to, Customer under the Agreement, Supplier shall maintain vulnerability and patch management processes and tools to regularly assess software for security vulnerabilities, and to deploy software patches and updates. Supplier shall provide updates, patches, and vulnerability alerts to Customer pertaining to software on a regular and timely basis. At a minimum, Supplier will inform Customer CISO and information security team (InfoSecOps@Discovery.com) within 24 hours of discovering security vulnerabilities in systems connecting to Customer information technology assets or systems provided to/developed for Customer by Supplier. Subject to an express provision to the contrary, Supplier shall provide a hotfix, patch, or workaround that mitigates the security risks arising from such vulnerabilities. Critical and high risk security updates shall be applied within seven days, and medium and low risk vulnerabilities shall be addressed within one month.
   e. If Supplier is providing software that will be managed by Customer – on-premises or in the cloud – such software shall be compatible with Customer's suite of cybersecurity tools.

10. **Removable Media and Maintenance Tools.** Supplier shall ensure that Service Provider Systems, Maintenance Tools, and Removable Media will remain free of Malware, now known or later discovered. Supplier shall create processes, introduce protection mechanisms, and train Supplier Personnel for the purpose of screening, inspecting, monitoring, identifying and immediately handling any Malware in the Removable Media and Maintenance Tools consistent with the terms of this Security Rider. Supplier shall inspect and check Maintenance Tools and Removable Media for Malware or unauthorized modifications before they are used

in Supplier Systems, Customer Systems or Customer Data. Supplier shall restrict use of Removable Media and Maintenance Tools to authorized Service Provider Personnel only. Supplier shall prevent unauthorized removal of Removable Media containing Customer Data by: (i) verifying that no Customer Data is stored on the applicable Removable Media, (ii) Sanitizing or destroying the Removable Media (such that Customer Data cannot be read or recreated); (iii) retaining the Removable Media within the facility in which it is being utilized; or (iv) requiring and obtaining explicit authorization to remove the Removable Media from the facility.

11. **PCI Compliance.** If applicable to the Services, Supplier and Supplier Personnel shall comply with, and ensure that, to the extent required under the Payment Card Industry Data Security Standard ("PCI DSS") located at www.pcisecuritystandards.org (as the same may be amended and supplemented from time to time), their applications, infrastructure, and technology that process, store, or transmit Customer Data or transaction-level data comply with the PCI DSS at all times. Further, any payment applications (as applicable) that process, store, or transmit Customer Data or transaction-level data must comply with the PCI Payment Application Data Security Standard ("PA-DSS") located at www.pcisecuritystandards.org (as the same may be amended and supplemented from time to time). With respect to Supplier's PCI DSS and PA-DSS obligations detailed above, Supplier shall provide Customer with: (i) an executive summary of a Report on Compliance ("ROC") performed by a Payment Card Industry Security Standards Council ("PCI SSC") certified Qualified Security Assessor ("QSA"); (ii) a completed Attestation of Compliance (contained within the PCI DSS Requirements and Security Assessment Procedures); (iii) a PCI PA-DSS Report on Validation (a "ROV") performed by a PCI SSC certified Payment Application Qualified Security Assessor ("PA-QSA"); and (iv) a completed Attestation of Validation for each payment application developed by Supplier or Supplier Personnel that processes, stores, or transmits Customer Data or transaction-level data as of the date Supplier implements the Services under this Agreement and, thereafter, upon Customer's reasonable request, but no more than once per year. Customer may share such information (including any reports) with its Affiliates and/or its regulatory authorities. In addition, in the event Supplier notifies Customer of a suspected or actual Security Incident, Customer may request a ROC within six (6) months of such notice, and Supplier shall provide such ROC to Customer.

12. **Audits and Reporting**

    a. Supplier shall monitor the effectiveness of its security program by conducting self-audits and risk assessments of the Supplier Systems against the written policies and procedures maintained by Supplier as required herein no less frequently than annually. Supplier shall be responsible for ensuring consistency of its security operations, including proactive monitoring and mitigation of vulnerabilities.
    b. Supplier shall use external auditors to verify the adequacy of its security measures on no less than an annual basis. Such audits: (a) will include testing of the entire measurement period since the previous measurement period ended; (b) will be performed according to AICPA SOC2 standards or such other alternative standards that are substantially equivalent to AICPA SOC2; (c) will be performed by independent third-party security professionals; and (d) will result in the generation of an audit report ("Report"). Reports will be made available to Customer upon request and will be treated as Confidential Information.
    c. During the Term, Customer reserves the right, with commercially reasonable notice to Supplier, to conduct a full security audit, including, but not limited to, penetration or vulnerability testing of Supplier's relevant networks, systems, and processes, to identify the strengths and weaknesses of Supplier's existing security controls and to ensure Supplier's compliance with this Agreement.

13. **Secure Destruction of Data.**

    a. Upon expiration or termination of the Agreement or upon written request by Customer, Supplier shall return to Customer and/or destroy any Customer Data in

Supplier's possession or control in accordance with the terms of the Agreement, and at all times pursuant to Customer's instructions.

b. Supplier shall ensure the secure disposal of Customer Data and any media or hardware containing Customer Data in accordance with National Institute of Standards and Technology (NIST) recommendations (or a successor standard widely used in the industry), and Supplier shall certify in writing to Customer that Customer Data has been destroyed in accordance with such standards.

14. **Non-US Customer Personal Data.** The following provisions in this Section shall apply only to the extent Supplier processes non-US Customer Data and in such instances, shall apply in addition to the other provisions in this Security Rider.

a. Supplier's written data security policies and procedures shall include: (a) the security policy applicable to the Services; and (b) internal manuals setting out how to use the Supplier Systems and how to secure Customer Data and/or Customer Systems, as applicable.

b. The Supplier shall give appropriate written instructions in advance, clearly specifying Supplier mechanisms to ensure that Customer Data and/or Customer Systems remain available in the event Supplier Personnel necessary to carry out certain Customer Data processing activities (i.e., with "need to know" access) are either absent or unavailable to an extent that would cause delays.

c. Supplier Systems shall provide functionality that allows a record to be kept of:

   i. The date when the Customer Data has been registered for the first time in the Supplier System;
   ii. an identifier of the user who registers the Customer Data in the Supplier System;
   iii. sources of Customer Data, if Customer Data have not been obtained from the data subject;
   iv. information on recipients ((i) to whom Customer Data have been disclosed; (ii) the date thereof; and (iii) the scope of this disclosure);
   v. modifications or relations made to Customer Data and the author of such actions; and
   vi. any objection of the data subject to the processing of their data.

d. If either the Customer Data or means of protecting the Customer Data have been damaged, the Supplier shall adopt suitable measures to ensure that Customer Data access is restored within a period which is compatible with data subjects' rights under Law, and in any event is not in excess of seven (7) days.

e. Where the Services involve managing Customer Data and/or Customer Systems on behalf of Customer, the Supplier shall appoint, in writing, a system administrator who oversees such activities. A list of the system administrators shall be kept by the Supplier for inspection by Customer on request at any time. The system administrators will be required to monitor access to the Customer Data and Customer Systems and keep a copy of log/access files for six (6) months, Supplier shall, on (at least) an annual basis, conduct an assessment on the activities of the system administrator.

Business Continuity and Recovery

CIRCUMSTANCES

Action is activated in response to an incident causing significant disruption to normal service delivery/business, particularly the delivery of key/critical activities. Examples of circumstances triggering activation of this Plan include:

- Loss of key staff or skills e.g. above normal levels of absenteeism due to illness
- Loss of critical systems e.g. ICT failure

- Denial of access, or damage to, facilities e.g. loss of a building through fire
- Loss of a key resource e.g. a major supplier vital to the delivery of a key service

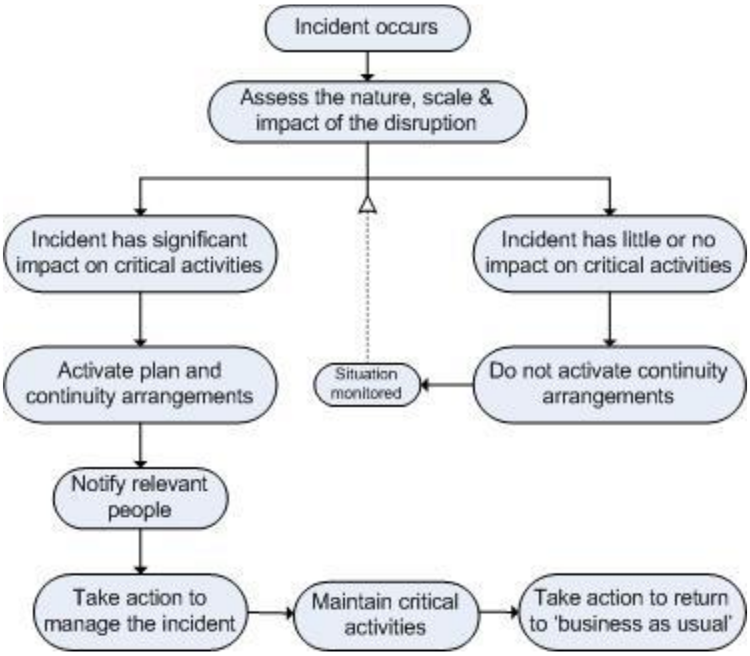
RESPONSIBILITY FOR ACTIVATION

A member of the nominated **Business Continuity Team**[1] for Village Software Engineering Limited will normally activate and stand down this Plan:

Name	Role	Office	Out of Office	Mobile
Johnny Read	Managing Director	0151 709 7728		
Ian Bufton	Technical Director	0151 709 7728		
Sue Roberts	Commercial Director	0151 709 7728		

[1] The group of staff who will come together to lead the response to a disruptive incident – usually senior staff within the team/service/organisation.

PROCESS FOR ACTIVATION


Incident occurs
Assess the nature, scale & impact of the disruption
Incident has significant impact on critical activities
Incident has little or no impact on critical activities
Activate plan and continuity arrangements
Situation monitored
Do not activate continuity arrangements
Notify relevant people
Take action to manage the incident
Maintain critical activities
Take action to return to 'business as usual'

Incident management

PURPOSE OF THE INCIDENT MANAGEMENT PHASE

- Protect the safety of staff, visitors and the wider community
- Protect vital assets e.g. equipment, data, reputation etc.
- Ensure necessary communication takes place
- Support the Business Continuity phase
- Support the Recovery and Resumption phase

ACTIONS TO PROTECT THE SAFETY AND WELFARE OF STAFF, VISITORS AND THE PUBLIC

The following actions will be taken to protect the immediate safety of staff, visitors and the public:

□[2]	ACTION	FUTHER INFO/DETAILS
1.	**Evacuate** the building if necessary	Use normal evacuation procedures for the building
2.	Ensure all staff report to the Assembly Point.	The **Assembly poi**nt for the Village Software Engineering Limited is: The Car Park, to the rear of the Tempest Building The **alternative Assembly Point** for the Village Software Engineering Limited is: Across the Road on Tithebarn Street Ian Bufton is responsible for completing this action
3.	Call emergency services (as appropriate)	TEL: 999 Ian Bufton is responsible for completing this action
4.	Check that all staff, contractors and any visitors have been evacuated from the building and are present. Consider safety of all staff, contactors and visitors as a priority	Check using sign in / sign out sheets and Calendar Ian Bufton is responsible for completing this action
5.	Ensure log of incident is started and maintained throughout the incident phase	Use a decision and action log to do this. The log template can be found Microsoft Teams -> General -> Policies -> Business Continuity
6.	Record names and details of any staff, contractors or visitors who may have been injured or distressed in the incident.	Ian Bufton is responsible for completing this action

□[2]	ACTION	FUTHER INFO/DETAILS
7.	Forward details of any fatalities or injuries in the incident to HR (depending on scale of incident) and agree action that will be taken.	The HR contact to forward this information to is Sue Roberts Sue Roberts is responsible for completing this action
8.	Assess impact of the incident to agree response / next steps	Sue Roberts is responsible for completing this action
9.	Log details of all items lost by staff, visitors etc. as a result of the incident	Sue Roberts is responsible for documenting this information
10.	Consider whether the involvement of other teams, services or organisations are required to support the management of the incident	Depending on the incident the following may be approached to assist with incident management: • Personnel • Health and Safety • Legal • Occupational Health

COMMUNICATION ACTIONS

In the event of an incident and this plan being activated, the following people should be contacted. Nature of contact will depend on the incident type and time it has occurred.

Sue Roberts is responsible for completing the communication actions.

ALWAYS CONTACTED

□	Name	Role	Contact Details	Likely message
1.	Johnny Read	Managing Director	read@villagesoftware.co.uk	▪ Incident is taking place ▪ Action being taken ▪ Impact on the service ▪ Request to escalate or support
2.				▪

CONTACTED DEPENDING ON INCIDENT

□	Name	Role	Contact Details	Likely message
1.	Sue Roberts	Comms Officer	Sue.roberts@villagesoftware.co.uk	▪ Incident is taking place ▪ Action being taken ▪ Impact on the service ▪ Indication of any press interest ▪ Areas they can support service

CONTACTED DEPENDING ON INCIDENT				
□	**Name**	**Role**	**Contact Details**	**Likely message**
2.	Ian Bufton	Staff	Ian.bufton@villagesoftware.co.uk	▪ Incident is taking place ▪ Action being taken ▪ Impact on the service ▪ Where they need to report to/work from
3.	Graham James	Key Suppliers	Graham.james@villagesoftware.co.uk	▪ Incident is taking place ▪ Action being taken ▪ Impact on the service ▪ Where they need to report to/work from
4.	Customers	N/A	Standard email sent to client contacts from within Dynamics365	▪ Incident is taking place ▪ Action being taken ▪ Impact on the service ▪ Expected duration of the disruption

ACTIONS TO SUPPORT BUSINESS CONTINUITY

□	ACTION	FUTHER INFO/DETAILS
1.	Recover vital assets/equipment to enable delivery of critical activities[3]	The essential equipment/resources/information that need to be recovered where possible are: Key assets held in Azure Recover details from impact assessment held in Microsoft Teams -> General -> Policies -> Business Continuity
2.	Assess the key priorities for the remainder of the working day and take relevant action	Consider sending staff home, to recovery site etc
3.	Inform staff what is required of them	Depending upon the event, staff would work from home or the clients' sites depending upon the type of work to minimise disruption.
4.	Publicise the interim arrangements for delivery of critical activities	Ensure all stakeholders are kept informed of contingency arrangements as appropriate Redirect phones and adjust message Issue arrangement emails to clients and suppliers Place a message on the website

ACTIONS TO SUPPORT RECOVERY AND RESUMPTION

	ACTION	FUTHER INFO/DETAILS
1.	Take any salvage/asset recovery actions that are appropriate	Remove any equipment, furniture, records etc. that are at risk of damage.
2.	Continue to log all expenditure incurred as a result of the incident	Use a financial expenditure log to record costs incurred as a result of responding to the incident
3.	Seek specific advice/ inform your Insurance Company	

COMMUNICATING WITH STAFF

Name	Role	Contact Details
Ian Bufton	Technical Director	Ian.bufton@villagesoftware.co.uk

[3] See 4.1 of this Plan for details of critical services

BUSINESS CONTINUITY

PURPOSE OF THE BUSINESS CONTINUITY PHASE

The purpose of the business continuity phase of response is to ensure that critical activities are resumed as quickly as possible and/or continue to be delivered during the disruption.

The Business Impact Analysis (BIA) for the Village Software Engineering Limited sets out details of critical activities and the resources required to deliver them both in 'business as usual' and in crisis situations. The Business Continuity Team[4] will refer to the BIA to help inform the business continuity response that is required.

CRITICAL ACTIVITIES

The outcome of the Business Analysis process has been to identify the following activities as critical:

	Brief Description of Critical Activities
1.	Client project delivery
2.	Product development
3.	Support and managed services
4.	Accounts receivable and payable

NON-CRITICAL ACTIVITIES

A number of activities are non-critical and consideration will be given to:

- Not recovering these activities until critical activities have been resumed
- Suspending these activities and diverting their resources to support the critical ones

The non-critical activities for this team/service/organisation are:

	Brief Description of Non-Critical Activities
1.	Marketing
2.	Sales and Business Development

[4] See Section 2 of this Plan for information on the Business Continuity Team

BUSINESS CONTINUITY ACTIONS

The Business Continuity Team (See Section 2) for the incident is responsible for ensuring the following actions are completed:

	ACTION	FUTHER INFO/DETAILS
1.	Identify any other staff required to be involved in the BC response	Depending on the incident, the Business Continuity Team may need additional/specific input to drive the recovery of critical activities
2.	Evaluate the impact of the incident	Use an incident impact assessment form to understand the impact of the incident on 'business as usual' working activities.
3.	Plan how critical activities will be maintained.	Consider: ▪ Immediate priorities ▪ Communication strategies ▪ Deployment of resources ▪ Finance ▪ Monitoring the situation ▪ Reporting
4.	Log **all** decisions and actions, including what you decide **not** to do and include rationale	Use a decision and action log to do this
5.	Log **all** financial expenditure incurred	Use a financial expenditure log to do this
6.	Allocate specific roles as necessary	Roles allocated will depend on the incident and availability of staff
7.	Secure resources to enable critical activities to continue/be recovered	Consider requirements such as the staffing, premises, equipment. *Refer to BIA for more detailed information on resource needs.*
8.	Deliver appropriate communication actions as required	Ensure methods of communication and key messages are developed as appropriate to the needs of your key stakeholders e.g. customers, suppliers, staff, Executive Boards, Shareholders etc.

RECOVERY AND RESUMPTION

PURPOSE OF THE RECOVERY AND RESUMPTION PHASE

The purpose of the recovery and resumption phase is to resume normal working practises for the Village Software Engineering Limited. Where the impact of the incident is prolonged, normal operations may need to be delivered under new circumstances e.g. from a different building.

RECOVERY AND RESUMPTION ACTIONS

	ACTION	**FUTHER INFO/DETAILS**
1.	Agree and plan the actions required to enable recovery and resumption of normal working practises	Agreed actions will be detailed in an action plan and set against timescales with responsibility for completion clearly indicated.
2.	Continue to log all expenditure incurred as a result of the incident	Use a financial expenditure log to do this
3.	Respond to any long terms support needs of staff	Depending on the nature of the incident, the Business Continuity Team may need to consider the use of Counselling Services e.g. internal Occupational Health involvement or appropriate External Agencies
4.	Carry out a 'debrief' of the incident and complete an Incident Report to document opportunities for improvement and any lessons identified	Use an Incident Report Form to do this. This should be reviewed by all members of the Business Continuity Team to ensure key actions resulting from the incident are implemented within designated timescales
5.	Review this Continuity Plan in light of lessons learned from incident and the response to it	Implement recommendations for improvement and update this Plan. Ensure a revised version of the Plan is read by all members of the Business Continuity Team
6.	Publicise that there is now 'business as usual'	Issue email to clients and suppliers Update message left on the website. Remove after 5 working days. Remove any phone message that was left.

Quality - Overview

Village Software places a high emphasis on the quality of the software products that we develop. In order to achieve this high standard we strive to deliver quality at all levels, implementing control on all aspects of our work from technical development, sales, administration, supplier evaluation and support.

QA process covers all stages of the product development.

We believe that good communication is the key to being able to deliver quality. This encompasses communication with clients and internally with the project team and other employees. Documents are managed by version control, records conform to filing procedures and any nonconforming products, corrective action and preventative action are all recorded and evaluated as part of project management.

We internally use back office systems to manage the task delivery process. JIRA is to be used for ongoing development for this purpose.

Development Procedures

For each project a testing strategy is defined. By default this will include unit testing in code and integration testing. The testing approach is used both to confirm delivery of required functionality and as a quality assurance technique associated with the release plan.

The test strategy should be recorded in the project record and will normally include unit and integration tests. It may also include tests across alternative platforms and stress tests where appropriate.

In order to check the product's quality the following tests may be included in the product plan performed:

- functionality tests
- usability tests (tests of consistency in the user interface, online and context-sensitive help, and user documentation)
- reliability tests (integrity tests, structure tests, and stress tests)
- performance tests

Where bugs are found in release candidates these are to be captured in the JIRA system. Ordinarily they will be added to the project backlog then moved through the cycle of selected for development, in progress and ready for release. They will then be tested in the release. If a bug is not fixed, then it remains a defect in the backlog. So our QA team provides defect tracking life cycle.

At the release stage bugs and other non conformance issues are identified as level 1,2,3. Level 1 are issues that prevent the functioning of the system, Level 2 are non conformances or bugs for which work around procedures can be used prior to being fixed. Level 3 are issues that while they degrade the system and are non conformant they do not require a work around.
Correction of these issues will then be scheduled against their priorities.

Release Procedures

Because product releases bring together complex components into a whole it is necessary to tightly control this part of the process to ensure quality.

Each project (or each component of a project as appropriate), will have a written release procedure. It is the responsibility of the Senior Developer assigned to the project to ensure that an up to date release procedure is in place.

It is the responsibility of the developer carrying out the release to ensure that the release procedure is adhered to and any variances are recorded.

While release procedures can vary depending on the nature of the project the following would be considered an ordinary approach.

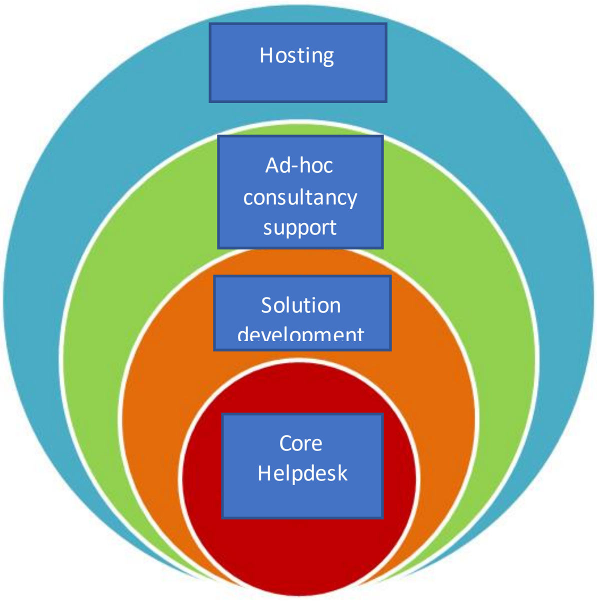
1. Code is extracted from sourcecontrol and the project built.
2. Changes (for example release numbers) suggested in checklist are updated.
3. Internal unit tests are run.
4. The system is released to the Quality Assurance System.
5. Integration including manual tests are run against the QA system.
6. Often clients are invited to run any testing they require on the QA system.
7. System is released from QA to live.
8. Relevant parties are informed.

Steps 1 to 4 and step 7 where possible should be automated, usually this is done using the Jenkins system. On occasions client requirements, for example release from their internal system where they don't have Jenkins or a similar continuous integration system, mean this cannot be automated. This should be noted in the release procedure.

Customer Satisfaction

Throughout the development process the customer will have regular communication with the Village account manager and/or development team as part of the project management process. This helps to ensure that expectations are met and leads to greater customer satisfaction. The account manager will confirm the satisfaction level of the customer both during development and after delivery. This also encompasses the administrative and financial office procedures.
We are constantly reviewing our procedures and practices in order to ensure quality and welcome suggestions for improvement.

Support Services:



Any solution developed by Village Software will be supported after "go live" and as shown in the diagram above there are 4 key elements to our support services and it is the mix of these elements that we bespoke for each client. Any element can be chosen by the Client and indeed any mix of the 4 elements.

Core helpdesk

Our helpdesk service is our on-line 2nd tier support services that operates between the hours of 9am and 5pm on weekdays excluding public holidays. This service is there to help clients to fix software issues and to help clients to understand how to use the solution correctly. If agreed Village are happy to include the remote updating and upgrading of software for the client within this core service. Equally if the client requires support beyond the above stated core hours, this can be agreed. The core helpdesk fee is agreed with the Client and is paid annually in advance.

Solution Development (Budget based consultancy)

This element covers a "pot of time" to add enhancements to the signed off solution with these enhancements and developments usually delivered via remote consultants. The pot of time is agreed annually in advance and the client typically draws time down from the agreed pot in 15 minute units. If the pot needs to be "topped up" during the year then the client can readily do this and equally if the original pot of time is not used within the year the balance can be taken into account when agreeing the pot of time for the next year. The value of the pot is paid monthly in advance.

Ad-hoc consultancy

In some cases Clients prefer to have their solution supported via ad-hoc on-site and remote consultancy service. Typically, an hourly rate is agreed with the Client and this rate is used for the consultancy time which is charged and paid monthly in arrears.

Hosting and Cloud

This element is used by Clients that require a fully managed service or the provision of a Cloud based solution. Village are happy to offer the platform and infrastructure as a service as well as the software solution and fully maintain the service to cover all of the Clients solution functionality requirements. A monthly "service" charge is agreed for 12 month periods and typically, as a Microsoft Gold partner and Cloud specialist, we utilise Azure as the Cloud Service.

Any Mix

As stated above a "mix" of any of the above works very well. The most common approach amongst our clients is to utilize the Core Helpdesk with the Solution development which in essence provides a "bureau" service to ensure your solution is fully supported while also allowing it to develop and grow, but within a controlled budget.

Whatever you choose we will work up a bespoke agreement with you and it is not fixed in "tablets of stone". We can change amend and adjustment throughout the year to ensure you always have a support arrangement that suits and evolves with your business.