

**RM6100 Technology Services 3 Agreement
Framework Schedule 4 - Annex 1
Lots 2, 3 and 5 Order Form**

Order Form

This Order Form is issued in accordance with the provisions of the Technology Services 3 Framework Agreement RM6100 between the Supplier (as defined below) and the Minister for the Cabinet Office (the "**Framework Agreement**") and should be used by Buyers after making a direct award or conducting a further competition under the Framework Agreement.

The Contract, referred to throughout this Order Form, means the contract between the Supplier and the Buyer (as defined below) (entered into pursuant to the terms of the Framework Agreement) consisting of this Order Form and the Call Off Terms. The Call-Off Terms are substantially the terms set out in Annex 2 to Schedule 4 to the Framework Agreement and copies of which are available from the Crown Commercial Service website [RM6100 Technology Services 3](#).

The Supplier shall provide the Services and procure the provision of Third Party Bullwall Software (Third Party COTS) specified in this Order Form (including any attachments to this Order Form) to the Buyer on and subject to the terms of the Contract for the duration of the Contract Period.

In this Order Form, capitalised expressions shall have the meanings set out in Schedule 1 (Definitions) of the Call-Off Terms

This Order Form shall comprise:

1. This document headed "Order Form";
2. Attachment 1 – Services Specification;
3. Attachment 2 – Charges and Invoicing;
4. Attachment 3 – Implementation Plan;
5. Attachment 4 – Service Levels and Service Credits;
6. Attachment 5 – Key Supplier Personnel and Key Sub-Contractors;
7. Attachment 6 – Software;
8. Attachment 7 – Financial Distress;
9. Attachment 8 - Governance
10. Attachment 9 – Schedule of Processing, Personal Data and Data Subjects;
11. Attachment 10 – Transparency Reports; and
12. Annex 1 – Call Off Terms and Additional/Alternative Schedules and Clauses.

The Order of Precedence shall be as set out in Clause 2.2 of the Call-Off Terms being:

- .1.1 the Framework, except Framework Schedule 18 (Tender);
- .1.2 the Order Form;
- .1.3 the Call Off Terms; and
- .1.4 Framework Schedule 18 (Tender).

Section A

General information

Contract Details

Contract Reference:

MEDWAY PO No.: 250015795
/
Ricoh Internal Sourcing Ref: 8720936695

Contract Title:

CCS RM6100 - Technology Services 3 - Lot 3b
- Bullwall

Contract Description:

Bullwall Ransomware Containment (Third Party COTS Software) – 4,500 AD User Licences
Related ancillary professional services at commencement – namely installation and training.

Contract Anticipated Potential Value: this £81,000.00, exc vat.
should set out the total potential value of the Contract

Estimated Year 1 Charges:

£81,000.00 exc VAT full sum payable up-front
(non-refundable firm sale)

Commencement Date: this should be the date of the 24/03/2025
last signature on Section E of this Order Form

Buyer details

Buyer organisation name

Medway NHS Foundation Trust

Billing address

Your organisation's billing address - please ensure you include a postcode

Windmill Road, Gillingham, Kent ME7 5NY

Buyer representative name

The name of your point of contact for this Order
Sarah Brissenden

Buyer representative contact details

Email and telephone contact details for the Buyer's representative. This must include an email for the purpose of Clause 50.6 of the Contract.

s.brissenden@nhs.net

Buyer Project Reference

Please provide the customer project reference number.

MFT Bullwall.

Supplier details

Supplier name

The supplier organisation name, as it appears in the Framework Agreement
Ricoh UK Ltd

Supplier address

Supplier's registered address
Head Office, 2nd Floor, 900 Pavilion Dr, Northampton NN4 7RG.

Supplier representative name

The name of the Supplier point of contact for this Order
David Blenkinsop, Government Strategic Account Director Cyber
Mobile: 07771 618494, david.blenkinsop@ricoh.co.uk

Supplier representative contact details

Email and telephone contact details of the supplier's representative. This must include an email for the purpose of Clause 50.6 of the Contract.

Ricoh UK, Head Office, 2nd Floor, 900 Pavilion Dr, Northampton NN4 7RG.
David Blenkinsop, Government Strategic Account Director Cyber, Mobile: 07771 618494
david.blenkinsop@ricoh.co.uk

Order reference number or the Supplier's Catalogue Service Offer Reference Number

A unique number provided by the supplier at the time of the Further Competition Procedure. Please provide the order reference number, this will be used in management information provided by suppliers to assist CCS with framework management. If a Direct Award, please refer to the Supplier's Catalogue Service Offer Reference Number.

1-1QKLN4TD

Guarantor details

Guidance Note: Where the additional clause in respect of the guarantee has been selected to apply to this Contract under Part C of this Order Form, include details of the Guarantor immediately below.

Guarantor Company Name

The guarantor organisation name

[Not Applicable]

Guarantor Company Number

Guarantor's registered company number

[Not Applicable]

Guarantor Registered Address

Guarantor's registered address

[Not Applicable]

Section B

Part A – Framework Lot

Framework Lot under which this Order is being placed

Tick one box below as applicable (unless a cross-Lot Further Competition or Direct Award, which case, tick Lot 1 also where the buyer is procuring technology strategy & Services Design in addition to Lots 2, 3 and/or 5. Where Lot 1 is also selected then this Order Form and corresponding Call-Off Terms shall apply and the Buyer is not required to complete the Lot 1 Order Form.

- | | |
|--|-------------------------------------|
| 1. TECHNOLOGY STRATEGY & SERVICES DESIGN | <input type="checkbox"/> |
| 2. TRANSITION & TRANSFORMATION | <input type="checkbox"/> |
| 3. OPERATIONAL SERVICES | |
| a: End User Services | <input type="checkbox"/> |
| b: Operational Management | <input checked="" type="checkbox"/> |
| c: Technical Management | <input type="checkbox"/> |
| d: Application and Data Management | <input type="checkbox"/> |
| 5. SERVICE INTEGRATION AND MANAGEMENT | <input type="checkbox"/> |

Part B – The Services Requirement

Commencement Date

See above in Section A

Contract Period

Guidance Note – this should be a period which does not exceed the maximum durations specified per Lot below:

| Lot | Maximum Term (including Initial Term and Extension Period) – Months (Years) |
|-----|---|
| 2 | 36 (3) |
| 3 | 60 (5) |
| 5 | 60 (5) |

Initial Term Months

18 Months

Extension Period (Optional) Months

N/A

Minimum Notice Period for exercise of Termination Without Cause no termination
without cause

Sites for the provision of the Services

Guidance Note - Insert details of the sites at which the Supplier will provide the Services, which shall include details of the Buyer Premises, Supplier premises and any third party premises.

The Supplier shall provide the Services from the following Sites:

Buyer Premises:

Medway NHS Foundation Trust, Medway Maritime Hospital, Windmill Road, Gillingham, Kent, ME7 5NY

Supplier Premises:

Ricoh Head Office, 2nd Floor, 900 Pavilion Dr, Northampton NN4 7RG

Third Party Premises:

BULLWALL Ltd, 8, The Courtyard, Furlong Rd, Bourne End SL8 5AU, UK

Buyer Assets

Guidance Note: see definition of Buyer Assets in Schedule 1 of the Call-Off Terms

Not Applicable

Additional Standards

Guidance Note: see Clause 13 (Standards) and the definition of Standards in Schedule 1 of the Contract. Schedule 1 (Definitions). Specify any particular standards that should apply to the Contract over and above the Standards.

Not Applicable

Buyer Security Policy

Guidance Note: where the Supplier is required to comply with the Buyer's Security Policy then append to this Order Form below.

Not Applicable

Buyer ICT Policy

Guidance Note: where the Supplier is required to comply with the Buyer's ICT Policy then append to this Order Form below.

Not Applicable

Insurance

Guidance Note: if the Call Off Contract requires a higher level of insurance cover than the £1m default in Framework Agreement or the Buyer requires any additional insurances please specify the details below.

Third Party Public Liability Insurance (£) - *[Not Applicable]*

Professional Indemnity Insurance (£) - *[Not Applicable]*

[Not Applicable]

Buyer Responsibilities**Goods**

Guidance Note: list any Goods and their prices.

Not Applicable

Governance – Option Part A or Part B

Guidance Note: the Call-Off Terms has two options in respect of governance. Part A is the short form option and Part B is the long form option. The short form option should only be used where there is limited project governance required during the Contract Period.

| Governance Schedule | Tick as applicable |
|---|-------------------------------------|
| Part A – Short Form Governance Schedule | <input checked="" type="checkbox"/> |
| Part B – Long Form Governance Schedule | <input type="checkbox"/> |

The Part selected above shall apply this Contract.

Change Control Procedure – Option Part A or Part B

Guidance Note: the Call-Off Terms has two options in respect of change control. Part A is the short form option and Part B is the long form option. The short form option should only be used where there is no requirement to include a complex change control procedure where operational and fast track changes will not be required.

| Change Control Schedule | Tick as applicable |
|---|-------------------------------------|
| Part A – Short Form Change Control Schedule | <input checked="" type="checkbox"/> |
| Part B – Long Form Change Control Schedule | <input type="checkbox"/> |

The Part selected above shall apply this Contract. Where Part B is selected, the following information shall be incorporated into Part B of Schedule 5 (Change Control Procedure):

- for the purpose of Paragraph 3.1.2 (a), the figure shall be £ N/A; and
- for the purpose of Paragraph 8.2.2, the figure shall be £ N/A.

Section C

Part A - Additional and Alternative Buyer Terms

Additional Schedules and Clauses (see Annex 3 of Framework Schedule 4)

This Annex can be found on the RM6100 CCS webpage. The document is titled RM6100 Additional and Alternative Terms and Conditions Lots 2, 3 and 5.

Part A – Additional Schedules

Guidance Note: Tick any applicable boxes below

| Additional Schedules | Tick as applicable |
|---|--|
| S1: Implementation Plan | <input type="checkbox"/> |
| S2: Testing Procedures | <input type="checkbox"/> |
| S3: Security Requirements (either Part A or Part B) | Part A <input type="checkbox"/> or Part B <input type="checkbox"/> |
| S4: Staff Transfer | <input type="checkbox"/> |
| S5: Benchmarking | <input type="checkbox"/> |
| S6: Business Continuity and Disaster Recovery | <input type="checkbox"/> |
| S7: Continuous Improvement | <input type="checkbox"/> |
| S8: Guarantee | <input type="checkbox"/> |
| S9: MOD Terms | <input type="checkbox"/> |

Part B – Additional Clauses

Guidance Note: Tick any applicable boxes below

| Additional Clauses | Tick as applicable |
|-----------------------------|--------------------------|
| C1: Relevant Convictions | <input type="checkbox"/> |
| C2: Security Measures | <input type="checkbox"/> |
| C3: Collaboration Agreement | <input type="checkbox"/> |

Where selected above the Additional Schedules and/or Clauses set out in document RM6100 Additional and Alternative Terms and Conditions Lots 2, 3 and 5 shall be incorporated into this Contract.

Part C - Alternative Clauses

Guidance Note: Tick any applicable boxes below

The following Alternative Clauses will apply:

| Alternative Clauses | Tick as applicable |
|--------------------------|--------------------------|
| Scots Law | <input type="checkbox"/> |
| Northern Ireland Law | <input type="checkbox"/> |
| Joint Controller Clauses | <input type="checkbox"/> |

Where selected above the Alternative Clauses set out in document RM6100 Additional and Alternative Terms and Conditions Lots 2, 3 and 5 shall be incorporated into this Contract.

Part B - Additional Information Required for Additional Schedules/Clauses Selected in Part A

Additional Schedule S3 (Security Requirements)

Guidance Note: where Schedule S3 (Security Requirements) has been selected in Part A of Section C above, then for the purpose of the definition of "Security Management Plan" insert the Supplier's draft security management plan below.

Not Applicable

Additional Schedule S4 (Staff Transfer)

Guidance Note: where Schedule S4 (Staff Transfer) has been selected in Part A of Section C above, then for the purpose of the definition of "Fund" in Annex D2 (LGPS) of Part D (Pension) insert details of the applicable fund below.

Not Applicable

Additional Clause C1 (Relevant Convictions)

Guidance Note: where Clause C1 (Relevant Convictions) has been selected in Part A of Section C above, then for the purpose of the definition of "Relevant Convictions" insert any relevant convictions which shall apply to this contract below.

Not Applicable

Additional Clause C3 (Collaboration Agreement)

Guidance Note: where Clause C3 (Collaboration Agreement) has been selected in Part A of Section C above, include details of organisation(s) required to collaborate immediately below.

Not Applicable

An executed Collaboration Agreement shall be delivered from the Supplier to the Buyer within the stated number of Working Days from the Commencement Date:

Not Applicable

Supplier Response

For the purpose of interpreting the applicable RM6100 framework terms, the Bullwall Ransomware Containment solution mainly consists of Third Party COTS Software operated by third party Bullwall, a non-affiliated supplier/partner to Ricoh UK.

In this respect Ricoh calls attention to clause 21.13 of the RM6100 framework terms as follows:

| | |
|---------|--|
| 21.13 | The Supplier shall: |
| 21.13.1 | notify the Buyer in writing of all Third Party COTS Software and Third Party COTS IPRs that it uses and the terms on which it uses them; and |
| 21.13.2 | unless instructed otherwise in writing by the Buyer in any case within twenty (20) Working Days of notification pursuant to 21.12.1, use all reasonable endeavours to procure in each case that the owner or an authorised licensor of the relevant Third Party COTS Software and Third Party COTS IPRs grants a direct licence to the Buyer on terms no less favourable (including as to indemnification against IPRs Claims) than those on which such software is usually made commercially available by the relevant third party. |

Bullwall is the licensor of the Third Party COTS Software in scope of this agreement, and pursuant to the above clause they have advised that the applicable terms of licence for the solution is located on the following website:

<https://bullwall.com/company/terms-conditions/>

Commercially Sensitive information

Any confidential information that the Supplier considers sensitive for the duration of an awarded Contract should be included here. Please refer to definition of Commercially Sensitive Information in the Contract – *use specific references to sections rather than copying the relevant information here.*

Not applicable

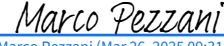
Section E

Contract Award


This Call Off Contract is awarded in accordance with the provisions of the Technology Services 3 Framework Agreement RM6100.

SIGNATURES

For and on behalf of the Supplier

| | |
|----------------|--|
| Name | Marco Pezzani |
| Job role/title | Customer Service Director |
| Signature |  <small>Marco Pezzani (Mar 26, 2025 09:31 GMT)</small> |
| Date | 26/03/2025 |

For and on behalf of the Buyer

| | |
|----------------|---|
| Name | Simon Wombwell Simon Wombwell |
| Job role/title | Chief Finance Officer Chief Finance Officer |
| Signature |  |
| Date | 25/03/2025 |

Attachment 1 – Services Specification
Attached overleaf

Attachment 1 – Services Specification

Proposal for

Ransomware protection

Prepared for:

**Medway NHS
Foundation Trust**

Growth Through Workstyle Innovation

Transform your work environment to enhance innovation and productivity

RICOH
imagine. change.

"We face a world of constant digital change that is redefining industries, markets and workplaces. Our purpose is to bring positive change to every organisation by empowering people and inspiring workstyle innovation. We believe there's always a better way."

Chris Hopton, CEO of Ricoh UK

"When designing the deployment Ricoh never came to us and said 'you've got a problem'. They worked with us, rather than for us and it felt like a partnership. Ricoh was flexible, we were flexible and together we delivered the project on time and on budget. I think that was the key thing for us really. We'll be upgrading the operating system on all desktops soon and it will be Ricoh that we'll turn to first to complete the work."

Spokesperson, International law firm

Our Founding Principles – Love your neighbour; Love your country; Love your work - were formulated in 1946 by our founder Kiyoshi Ichimura. They form the cornerstones of how we do business and encourage us to constantly improve and contribute to the wellbeing of all stakeholders - including our families, customers, and society as a whole.

By adhering to our management philosophy, we remain true to social and environmental sustainability and our responsibility to future generations.



Prince's Trust



FTSE4Good

Table of Contents

| | |
|---|-------------------------------------|
| About Ricoh. | 14 |
| Executive Summary | 5 |
| Ricoh <u>RansomCare Protection</u> | 6 |
| How Does RansomCare Work..... | 16 |
| Key Features..... | 18 |
| Detect..... | 19 |
| React..... | 19 |
| Respond..... | 19 |
| Recover..... | 20 |
| GDPR..... | 21 |
| Integration | 22 |
| Commercial Summary | 25 |
| Proposal For Medway NHS Foundation Trust..... | 25 |
| Notes | 26 |
| Post Implementation Support..... | 27 |
| Services | 27 |
| Availability | 27 |
| Document Quality Control..... | 29 |
| General Terms | Error! Bookmark not defined. |
| Ricoh's Portfolio of Services | Error! Bookmark not defined. |

About Ricoh

Ricoh is a global technology business and through organic and acquisitive growth has built a sizeable multi-vendor I.T. services organisation in Europe and internationally. Positioned as No.18 in CRN's 2024 UK top 100 I.T. reseller rankings by revenue and by Gartner in the Magic Quadrant for Managed Workplace Services in Europe (2024). Ricoh excels in integrating and managing solutions from multiple technology vendors, offering one of Europe's largest fleets of engineering workforces supporting global on-site deployments and in house 24/7/365 Service Operations Centres.

On its own, Ricoh IT Services accounts for 40% of Ricoh's Global Business and continues to grow as we transform into a Digital Services organisation.

We address your concerns by analysing your specific business objectives to identify the right solution that is agile, scalable and robust to support both your immediate and future business needs that deliver the right outcomes and most of all the best user and customer experience.

Our team of 476 UK based engineers help to support businesses with their technology infrastructure across multiple locations and countries. We also support modern working strategies with the latest technologies and help your organisation fully adopt collaboration tools to connect your people and drive productivity.

We constantly review, update and expand our portfolio of innovative products and services to help our customers stay ahead in an exceptionally challenging and dynamic field.

The Imagine. Change. methodology at Ricoh enables us to help our customers to maximise existing investments as well as design and deliver reliable, repeatable, efficient and high-quality services tailored to their unique and specific needs.

.

Executive Summary

According to leading research agencies Cybercrime is growing at an exponential rate and could cost the world economy up to \$10.5 Trillion annually by the end of 2025.

Data breaches expose sensitive information that can ruin companies' reputations and leave the organisation liable for compliance and regulatory violations. This can have a direct and significant impact on jobs, economic growth and investment.

With Cyber criminals finding more innovative and sophisticated ways to carry out attacks they are successfully bypassing traditional perimeter and endpoint security solutions. This has been exacerbated by the COVID19 pandemic and the necessity for organisations to allow their staff to work from home. With more organisation now also offering a hybrid workplace model which mixes in-office and remote work to offer flexibility and support to employees, this has led to the creation of a much larger attack surface and introducing more ways in which security can be compromised.

With ever-growing risk and weekly reports of Ransomware breaches in high profile organisations who have invested significantly in Perimeter and EDR IT Security solutions, Medway NHS Foundation Trust require a solution that will complement a traditional approach, providing a last line of defence in the event an attack successfully bypasses all other security measures.

An investment of £81,000.00 for an 18-month license will help to ensure that your organisation will remain compliant to financial, GDPR and government legislation and regulations. Your data will be more secure, the potential for reputational damage will be reduced and systems availability maintained.

RICOH RANSOMCARE (RC) PROTECTION

Why Ransomware Should Matter to You

Ransomware has evolved into enterprise-grade malware that holds computers and data files hostage, locks down entire systems swiftly and brings business to a halt for days, weeks or even months on end. Criminals are developing new methods continuously to defeat traditional methods of detection. Now more than ever, the C-suite (CIO, CISO CFO and CEO) has a significant responsibility to securely manage data and intellectual capital, to protect personally identifiable information, revenue, maintain customer loyalty and secure shareholder value.

It's critical that organisations do not rely solely on a reactive response to modern malware threats.

- According to the 2022 Cyber Security Breach Survey, 63% of disruptive breaches were reported by staff, not technology which is an alarming percentage bearing in mind the UK spent in excess of £4bn on cyber security solutions and services in 2022.
- Critical vulnerabilities are still being identified which allowed attackers to freely distribute ransomware. It can take several weeks for a viable, working fix to be distributed

When you consider the above, whilst Perimeter and Endpoint-based security solutions are an important part of the security toolset, they are not guaranteed to be fully effective against the proliferation and sophistication of new Cyber-attacks.

Our recommended strategy focuses on business continuity and disaster recovery with a last line of defence solution for Ransomware containment. This should include automatic alerting, shutdown response and quick recovery in order to avoid the vast costs often associated with ransomware attacks.

How Does RansomCare Work

BullWall came out of NC3 - The National Cyber Crime Centre in Denmark. It is an innovative technology that provides a 24/7 automated containment solution against ransomware attacks with inbuilt GDPR reporting. RansomCare (RC) is a unique, new technology with advanced multi-layered detection and with a completely different approach to threat prevention.

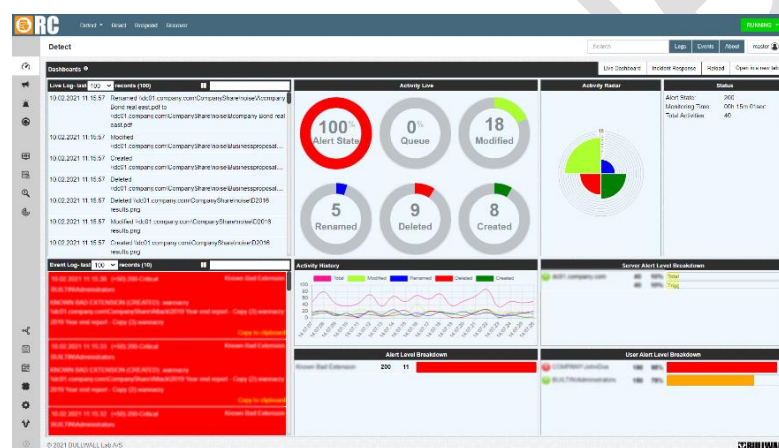
With a rapidly expanding attack surface to defend and multiple entry points for malware today, it does not matter which user or device triggered the attack. Nor does it matter if it is a known or unknown ransomware attack, or if the attack started on an endpoint, a mobile phone, an IOT device, via email, website drive-by-attack, instant messaging

app, USB key or cable, download, or was deployed maliciously by someone inside your organisation.

Even new and unseen ransomware will be detected, and the infected PC's shut down because RC is monitoring the impact of the file changes caused by ransomware rather than the malicious code itself. Furthermore, RC detects even whitelisted applications malicious tracks, which might be a result of insider or external activities with escalated privileges on a compromised network.

Every time someone creates a new file or overwrites an existing file – RC looks directly into the file and can see if any encryption has taken place. Multiple detection methods are employed to spot file changes within the data being saved.

When RC detects a ransomware attack, an alert will trigger the responses set up to isolate the user and/or device causing the encryption, stopping it immediately. The device can be shut down and the user can be disabled in AD (on-prem/cloud) so they cannot log onto another device to prevent the outbreak propagating further. RC also handles virtual environments like Citrix servers/sessions, Terminal servers/sessions, Hyper-V, VMware and the Cloud including Azure and Amazon AWS/EC2, SharePoint, Google Drive and Office 365.



The RC detection technology operates with event-based file detection, using more than 25 high-performance detection sensors to inspect the heuristics no matter the file. Every time someone creates a new file or modifies an existing file – RC looks directly into the file and can see if any encryption has taken place.

RC analyses existing file traffic on your network, resulting in minimal performance overhead – and RC is installed on a dedicated server, meaning it's agentless; this makes installation and deployment fast and easy with limited costs associated.

With a rapidly expanding attack surface to defend and multiple entry points for malware today, it does not matter which user or device triggered the attack. Nor does it matter if it is a known or unknown ransomware attack, or if the attack started on an endpoint, a mobile phone, an IOT device, via email, website drive-by-attack, instant messaging

app, USB key or cable, download, or was deployed maliciously by someone inside your organisation.

Even new and unseen ransomware will be detected, and the infected user/device is isolated because RC is monitoring the impact of the file changes caused by ransomware rather than the malicious code itself.

Key Features

- Instantly detect an ongoing ransomware outbreak
- Immediately detect and identify the user and client which initiated the encryption isolate the user/device
- RC is Agentless with negligible network or performance overhead
- Stop the ransomware in its tracks by using our built-in scripts (Shutdown device, disable user in Active Directory, terminate a Citrix session or disable network devices)
- Quickly identify the user and the files that have been encrypted for an easy restore from backup
- Automate your GDPR reporting

.2 DETECT

DETAILED LIVE VISIBILITY WITH PLAYBACK

RC creates a baseline of all the activity on your systems and in your environment. It simply monitors the network traffic going to and from your network file servers, using heuristics and metadata to discover ransomware swiftly. Artificial Intelligence and Machine Learning automates the alert settings, making it ever more sensitive based on your real network activity

In seconds, RC provides you with full visibility of any live file changes on your

The WEB Dashboard displays the recording log of any file creation, change, rename or deletion so should an attack occur you know exactly which files have been compromised. In case of an attack, you also have an advanced playback feature of the history log which enables you to easily study all related details.

No other security solution provides you with such a detailed and structured overview.

.3 REACT

RC STOPS THE ATTACK DEAD IN ITS TRACKS

RC will react within seconds of an unexpected file encryption taking place, alerting the Security Operations Centre (SOC) team, the attacked user, any other key stakeholders. The platform can also notify the local GDPR Supervisory Authority (SA) if required.

Alerting is done via email, SMS, IOS/Android app and through integration with most SIEM solutions. The alerting and communication will work if you are hosting in the cloud or if an MSP takes care of your IT solution and infrastructure.



.4 RESPOND

KEEP YOUR ORGANISATION RUNNING SMOOTHLY

RC will respond within seconds of any detected ransomware attack, shutting down the infected user/client and stopping the ransomware from spreading within the organisation. RC will inform you as soon as the attack has been stopped, and the alert level has returned to normal.

Integration through RESTful API to other security solutions such as Cisco ISE and Windows Defender ATP, means your security teams can unify security management across an increasingly complex sea of endpoints. RC provides a full damage report, listing all files or folders you need to recover from backup for speedy recovery of the few infected files that were compromised. With immediate response and a minimum number of files encrypted, it substantially removes the risk of a data breach according to GDPR.

.5 RECOVER

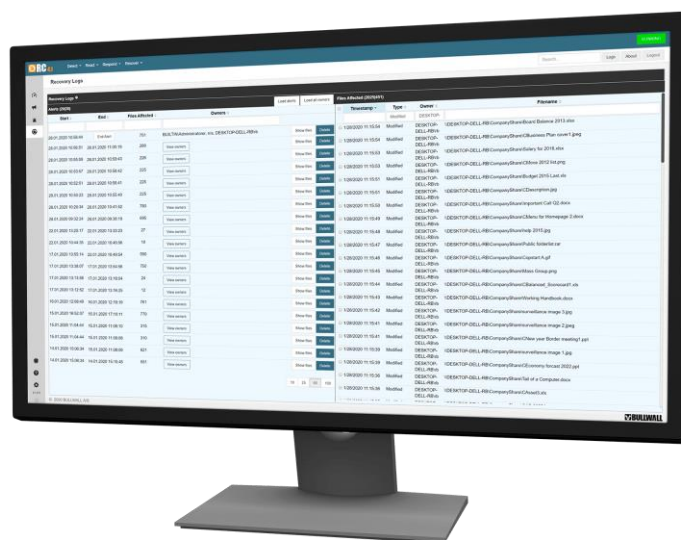
REMOVE PRESSURE FROM THE OPERATIONAL TEAM

RC enables rapid data-recovery. It gives you an exact list of the few files encrypted before the forced shutdown, that need to be restored from your backup. Identifying the exact files that need to be recovered will reduce any potential downtime saving you valuable time with minimal cost of recovery.

Some of the latest tactics from the cyber criminals include encrypting files without even changing the file name as well as encrypting files in different folders across your infrastructure.

This makes recovery difficult and ultimately forces you to restore a full backup, putting additional pressure on the entire organisation with operational loss and potentially a GDPR headache.

With RC your organisation can safely and quickly be operational without having to pay the ransom.



AUTOMATE YOUR GDPR RESPONSE WHEN HIT BY RANSOMWARE

According to the GDPR regulations: “If it’s likely that there will be a risk, then you must notify the local GDPR Supervisory Authority (SA); if it’s unlikely then you don’t have to report it. However, if you decide you don’t need to report the breach, you need to be able to justify this decision so you should document it”

Ransomware is an obvious tool of choice for cyber criminals, encrypting files on different shares and folders spread across the network, making GDPR reporting a challenge. Time pressure is now a serious issue, not only from the cyber criminals – but now you also only have 72 hours to comply with GDPR.

WITH GDPR, IT IS EITHER A MINOR INCIDENT OR A MAJOR BREACH

If you have a breach and have RC in place, it will mostly be a minor incident, but you still need to document your findings. RC provides a fully automated process for internal audit and for major breaches.

“A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, e.g., when it has been encrypted by ransomware, or accidentally lost or destroyed.”

With RC’s immediate response, most incidents will be considered minor, as only a few files will be compromised before a forced shut down. Customised GDPR reporting ensures you are compliant.

RC GDPR AUTOMATIC REPORTING PROVIDES

- ✓ Records of the exact time of the attack (beginning to end)
- ✓ Where the attack was initiated (which endpoint)
- ✓ Exactly which files have been affected
- ✓ Ownership of the file
- ✓ Details of how and when the breach was stopped
- ✓ Generates an incident report to key stakeholders

.7 INTEGRATION

RC can be integrated two ways to almost any SIEM and Network Access Control (NAC) solution. RC has a full featured RESTful WebAPI which can be easily adapted and setup, as it comes with pre-configured scripts for most common SIEM and NAC solutions. Setting up an integration to Cisco ISE, Aruba, Splunk, IBM QRadar, ATP and other solutions can in most cases be done in less than an hour.

When RC detects a ransomware attack, RC will immediately alert and send information to integrated solutions.

In case of using SIEM integration e.g. Splunk, RC will use JSON files sent to sensors in Splunk through TCP/Port listeners or through file integration. This will immediately trigger an alert in Splunk that will follow the workflow which is configured in Splunk for your Security Operations Centre (SOC) or Response Team to take appropriate action.

In case of using NAC integration to for e.g., Cisco ISE, RC will use the "ANC_Policy Quarantine" using XML to send to Cisco ISE WebAPI which immediately will isolate the attacked client/user from the network and the attack will instantly stop.

Setting up integration in RC is optional and not required. You decide if RC should Alert and Respond, if you prefer you can use your existing solutions instead, or a combination of the two.

All integration, communication and alerting functions also work if you are hosting in the cloud or if an MSP takes care of your IT solutions and infrastructure.



.8 Bullwall Server Intrusion Protection

Ransomware attacks have become a pervasive and costly threat to organizations worldwide. Among the various attack vectors leveraged by cybercriminals, one stands out: Remote Desktop Protocol (RDP).

Why RDP is Targeted For Ransomware Deployment

1. **Widely Used:** RDP is a legitimate and widely used technology for remotely accessing and managing Windows systems. Many organizations use it to enable remote work, provide technical support, and manage servers. Its ubiquity makes it an attractive target for attackers because it provides a direct pathway into a network.
2. **Weak or Default Credentials:** Attackers often find RDP servers with weak or default credentials. This can be due to poor password management, failure to change default passwords, or the use of easily guessable passwords. Attackers use tools that automate brute-force attacks to guess passwords and gain access to RDP services.
3. **Credential Theft:** Attackers may obtain RDP credentials through various means, such as phishing, keyloggers, or credential dumping attacks. Once they have valid credentials, they can easily access systems and deploy ransomware.
4. **Vulnerabilities and Exploits:** Vulnerabilities in RDP implementations can be exploited to gain unauthorised access to systems. Attackers can exploit these vulnerabilities to execute code remotely, which allows them to compromise systems without the need for valid credentials.
5. **Lateral Movement:** Once inside a network through an RDP compromise, attackers can move laterally to other systems and escalate privileges, making it easier to deploy ransomware across a broader range of systems.
6. **Lack of Monitoring and Logging:** In some cases, organizations may not have robust monitoring and logging in place for RDP sessions. This makes it difficult to detect and respond to unauthorised access until it's too late.

Extent of the Problem:

The extent of the RDP-based ransomware problem has been significant, with numerous reported cases of ransomware attacks leveraging RDP as an initial entry point. This issue is not confined to a particular region; it affects organisations on a global scale.

The **optional** Bullwall Server Intrusion Protection (SIP) module will detect unauthorised RDP sessions, alert and block the compromised clients and servers.

STOP THE RANSOMWARE DEPLOYMENT PROTOCOL



Contain Intrusion

By preventing unauthorized access, a containment protocol is implemented which prevents ransomware deployment, data encryption and data exfiltration.



Halt Breach Progression

By impeding reconnaissance and lateral movement, the potential for compromise in other network areas is effectively halted.



Defend Against Stolen Credentials

Including an MFA challenge substantially reduces the threat of unauthorized access, even with compromised credentials.

Confidential

COMMERCIAL SUMMARY

Proposal for Medway NHS Foundation Trust
RansomCare (RC) and Server Intrusion Protection (SIP)

| Ptem | Description | Total Cost |
|-----------------------------|--|------------|
| Pricing based on 4500 users | | |
| 1 | Bullwall (Third Party COTS) Software for licence duration of 18 Month inc. post implementation support for the duration of the term. | £81,000.00 |
| 2 | Installation and Training Services to be delivered by Ricoh | Included |
| | 18 Month Total | £81,000.00 |

NOTES

- Pricing:** ➤ All pricing is in GBP and is based on the quoted number of AD users.
- Term:** ➤ The license shall be granted for a duration of 18 months.
- The provided license key will be valid for the entirety of the chosen term.
- The license subscription period starts from date of installation to be determined and agreed.
- Delivery:** ➤ Date to be determined and agreed.
- The software is delivered electronically together with the license key
- Additional Terms:** As the software in scope is Third Party COTS Software pursuant to the RM6100 framework terms, the third party licensor's terms of licence applies as regards this COTS Software located at the following website:
<https://bullwall.com/company/terms-conditions/>

POST IMPLEMENTATION SUPPORT

Post Implementation support is provided directly by Bullwall and is inclusive in the costs shown. An overview of cover is provided below.

Services

Bullwall provides the following technical support for the RC supplied Software.

- Technical assistance for the operator
- Troubleshooting of software defects
- Update of the RC application
- Provision of 'known bad signature' updates*

* Within the RC software, the known bad signatures update every occurs 15 minutes throughout the day (default setting). This is an automated process provided that the RC Server has access to the RC Backend Server/Endpoint in the cloud.

Availability

Bullwall operate an online support ticket system at: <https://bullwall.com/support/>
The web-based support monitoring service is dynamic, so you can elect to increase the type and set priority via the web. Onsite support can be provided at the customer's expense.

Support tickets will receive a response based upon an assigned priority as follows:

- **Critical (1):** An Issue pursuant to which all or a substantial portion of the Software is not operating and cannot be restarted.
- **High (2):** An Issue which is responsible for a material portion of the Software not operating in substantial conformity with the applicable specifications.
- **Medium/Low (3,4):** A minor defect in the functionality of the Software

Bullwall will initiate a response as quickly as possible and initiate problem resolution, but there is no guaranteed response and resolution time depending on the issue. All workaround, resolution, and feedback/update activities will be provided relative to queues and prioritisation. Identification of priority and SLA timers depend on your issue and may be changed by Bullwall. Helpdesk staff provides support during normal business hours, excluding holidays, Monday through Friday. High availability and faster support response times can be purchased according to requirements. Under certain circumstances, Bullwall will put the problem resolution on hold – for example, when awaiting additional requested information from operator or approval for work that may have a temporary impact.

When raising a support ticket, you must provide Bullwall with detailed information about any suspected error(s), including an example, the context in which it was encountered, details of your system configuration, and the steps necessary to generate or reproduce the error. The priority level of a support ticket shall be determined by Bullwall at its sole discretion.

A detailed Service Level Agreement (SLA) is attached below.

Confidential

DOCUMENT QUALITY CONTROL

Document History

| Name | Date | Version No. | Comments |
|----------------|----------|-------------|--------------|
| Ellis Mitchell | 11/02/25 | V1.0 | New Document |
| | | | |

Document Quality Assurance

| Checked by | Date | Version No. | Actions |
|------------|----------|-------------|------------|
| Colin Lock | 11/02/25 | V1.0 | Peer Check |
| | | | |

Distribution

| Craig Allename | Date |
|----------------|----------|
| Craig Allen | 11/02/25 |
| | |
| | |
| | |
| | |
| | |



Crown
Commercial
Service

Attachment 2 – Charges and Invoicing

Part A – Milestone Payments and Delay Payments

| # | Milestone Description | Milestone Payment amount (£GBP) | Milestone Date | Delay Payments (where Milestone) (£GBP per day) |
|----|-----------------------|---------------------------------|----------------|---|
| M1 | N/A | N/A | N/A | N/A |
| M2 | | | | |
| M3 | | | | |
| M4 | | | | |
| M5 | | | | |

Part B – Service Charges

| Charge Number | Service Charges |
|------------------|-----------------|
| [Service Line 1] | |
| [e.g. SL1C1] | |
| [Service Line 2] | |
| [e.g. SL2C1] | |

Part C – Supplier Personnel Rate Card for Calculation of Time and Materials Charges

| Staff Grade | Day Rate (£) |
|-------------|--------------|
| | |
| | |



Crown
Commercial
Service

Part D – Risk Register

| Column 1 | Column 2 | Column 3 | Column 4 | Column 5 | Column 6 | Column 7 | Column 8 | Column 9 | Column 10 | Column 12 |
|-------------|-----------|---------------------|----------|------------|------------|----------------------|--------------------------|--------------------|----------------------------|-----------|
| Risk Number | Risk Name | Description of risk | Timing | Likelihood | Impact (£) | Impact (description) | Mitigation (description) | Cost of mitigation | Post-mitigation impact (£) | Owner |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |

Part E – Early Termination Fee(s)

N/A



Attachment 3 – Outline Implementation Plan

| # | Milestone | Deliverables (<i>bulleted list showing all Deliverables (and associated tasks) required for each Milestone</i>) | Duration (Working Days) | Milestone Date |
|----|------------------------------|--|----------------------------|----------------|
| M1 | [Concept Design] | [Statement of Requirements System/Application Specifications Interface Specifications Systems Testing Strategy Implementation Strategy and Plan Risk and Issues Management Plan Outline Disaster Recovery Plan Project Schedule Service Management Plan] | | |
| M2 | [Full Development] | [Design Verification Reports Design Validation Reports Change Management Plan System/Application Implementation Plan Risk and Issues Management Project Schedule Service Management Plan] | | |
| M3 | [System User Testing] | [System Test Report Risk and Issues Management Plan Project Schedule Service Management Plan Defects Log Final Inspection and Testing Report] | | |
| M4 | [User Readiness for Service] | [Training Plan Risk and Issues Log Implementation Plan Operations Plan Data Conversion & Cutover Plan Project Schedule Service Management Plan] | | |
| M5 | [Implementation] | [Implementation Plan Training Scripts] | | |
| M6 | [In Service Support] | [Post Implementation Report Data Conversion and Cut-Over Plan Service Delivery Reports Risk and Issues Log Service Management Plan Defects Log] | | |



Crown
Commercial
Service

Attachment 4 – Service Levels and Service Credits

Service Levels and Service Credits

Service levels for the Software overleaf

Service credits n/a

Service Credit Cap

N/A

Critical Service Level Failure

N/a

Bullwall Service Level Agreement (SLA)

1. Introduction

This Service Level Agreement (“SLA”) is an agreement between BullWall and Customer, including YOU as (“RC Operator”), to cover all the technical services and support provided by BullWall to RC Operator. This SLA includes a description of the technical services and support provided by BullWall to the dedicated RC Operator. The SLA is provided free of charge and is part of any Customer’s paid subscription during the term of the subscription.

Definitions of terms in SLA:

BullWall: The software manufacturer, distributor and service center for the RC Software.

BullWall Ransomware Containment Solution; Software: The Software BullWall provides is also referred to as (“RC”) or (“RC Software”) or (“Software”), which is the Software installed in your environment.

Customer: The end-user using and having the Software installed under accepted EULA.

RC Operator: A dedicated superuser (Customer or 3rd party) of the BullWall Ransomware Containment Solution Software supplied by BullWall. The RC Operator is expected to have received full training and must also have participated in implementing the BullWall Ransomware Containment (“RC”) solution. Services and support are not provided to any RC operator or users who have not taken training or taken part in the implementation.

Ticket or Support Ticket: An online Support Request via <https://bullwall.com/support>.

2. Software

Support Requirements: BullWall is an agentless technology implemented on existing infrastructure, making implementation safe and hassle-free; it is not an application that requires a daily Operator. BullWall monitors your connected file shares and protects your critical data by overlooking all file creations/changes happening



Crown
Commercial
Service

on the monitored file server shares. After installation, the Operator must have a system in place that warns if the BullWall software monitoring services are disabled or disconnected.

3. Services

BullWall provides the following technical support for the RC supplied Software.

- a. Technical assistance for the RC Operator.
- b. Troubleshooting of software defects.
- c. Update of the RC application, if any.

To obtain and initiate services and/or support you must raise an online Support Ticket at: <https://bull-wall.com/support/>.

BullWall has no official support phone number to call. Once you raise a Ticket, BullWall will contact you via e-mail to arrange a meeting or conversation if necessary.

4. Raising a Support Ticket

To request support, submit your support request on the online support ticket system at: <https://bull-wall.com/support/>. Our web-based support monitoring service is dynamic, so you can elect to increase the type and set priority via the web. Onsite support can be provided at the Customer's own cost.

When notifying BullWall of any support ticket, you must provide BullWall with detailed information (as requested in the example below) about the suspected issue, including an example (URL and complete screenshots), the context in which it was encountered, details of your system configuration, and the steps necessary to reproduce the issue. BullWall shall determine the priority level of a support ticket at its sole discretion.

SUBMIT A TICKET

Support tickets will be responded to according to priority.
Supported versions include BullWall 4.4.0.0 and onward.

First Name*

Last Name*

Email*

Company*

Message

Priority*

☒ Low Priority: 3 business days

☐ Medium Prio: 3 business days

☐ High Prio: 1 business day

☐ Critical Prio: 1 business day

Please Provide Screenshots

Drop files here or
SELECT FILES

Accepted file types: jpg, png, pdf, gif. Max. file size: 500 MB.

SUBMIT

Screenshot from Support Form: <https://bullwall.com/support>



Crown
Commercial
Service

After raising a support ticket, you will receive an email with a confirmation and a support ticket number for your reference.

5. Response Times

All web-based and logged support tickets to the Helpdesk will receive a response based on assigned priority:

- a. Critical Priority Issue (1): An issue pursuant to which all or a substantial portion of the Software is not operating and cannot be restarted.
- b. High Priority Issue (2): An issue that is responsible for a material portion of the Software not operating in substantial conformity with the applicable specifications.
- c. Medium/Low Priority Issue (3,4): A minor defect in the functionality of the Software or a related question.

BullWall will meet the following action times in the event of an issue.

| Priority Definition | Acknowledgment of Receipt | Workaround Solution | Resolution | Feedback/Update |
|---|---------------------------|---------------------|-----------------|---------------------------|
| Critical Priority Issue (1) High Priority Issue (2) <i>Prevents execution of the Software's objective.</i> | 45 mins | 1 Business Day | 5 Business Days | 1 Business Day (minimum) |
| Medium Priority Issue (3) Low Priority Issue (4) <i>Issues in the Software which have a moderate impact</i> | 2 hours | 3 Business Days | 8 Business Days | 3 Business Days (minimum) |

BullWall will initiate a response as fast as possible and initiate problem resolution, but there is no guaranteed response and resolution time depending on the issue. All workaround, resolution, and feedback/update activities will be provided relative to queues and prioritization. Identifying priority and SLA timers depends on your issue and may be changed by BullWall. Helpdesk staff provides support during normal business hours, excluding holidays, Monday through Friday. High availability and faster support response times can be purchased according to requirements. Under certain circumstances, BullWall will put the problem resolution on hold – for example, when awaiting additional requested information from the Operator or approval for work that may have a temporary impact.



6. Customer Responsibilities

The Customer's responsibility is that the appointed RC Operator has undertaken the necessary training in RC and has the appropriate skills and the necessary understanding for the Software operating the Customer's infrastructure. The RC Operator must have participated in the implementation of the Software.

The RC Operator must make sure all alert settings/information are updated within RC according to the Customer environment, such as email addresses for admin, alerts, response scripts, etc.

The RC Operators' responsibility is also to make sure settings in RC are updated accordingly if changes are made to any infrastructure, including but not limited to; Servers, Storage platforms, DFS, AD, DNS, or otherwise change settings that RC is dependent on for being fully operational. It is advised to conduct a monthly or quarterly isolation test monthly or quarterly either automatically or manually.

The RC Operators are responsible for raising a support ticket with the appropriate description described in this SLA.

BullWall shall be under no obligation to furnish support for the RC Software to the extent that such Support is necessary or desired as a result of (i) the operation of the RC Software in environmental conditions or configurations outside those initially implemented; (ii) your failure to upgrade or update the RC Software within a supported version as specified at: <https://bullwall.com/support/>; (iii) actions of any third party other than BullWall or a third party authorized by BullWall; and (iv) causes unrelated to the RC Software as delivered to you by BullWall, including without limitation, unauthorized modifications to the RC Software, made by you or on your behalf.

7. Software Updates

The "known bad signatures" update within the RC software every 15 minutes throughout the day (standard setting). This is an automated process provided the RC Server can access the RC Backend Server/Endpoint in the cloud.

RC Software upgrade notifications will be sent to the Admin email address defined in the RC settings.



Crown
Commercial
Service

8. Force Majeure

BullWall shall not be in breach of this Agreement, nor liable for any failure or delay in performance of any obligations under this Agreement arising from or attributable to acts, events, omissions, or accidents beyond its reasonable control (Force Majeure Event), including but not limited to any of the following:

- Fire, flood, earthquake, windstorm, or other natural disaster.
- War, threat of or preparation for war, armed conflict, imposition of sanctions, embargo, breaking off diplomatic relations, or similar actions.
- Terrorist attacks, civil war, civil commotion, or riots.
- Collapse of building structures, computers, or infrastructure.
- any labor dispute, including but not limited to strikes, industrial action, or lockouts.

BullWall shall use all reasonable endeavors to mitigate the effect of the Force Majeure Event to carry out its obligations under this Agreement in any way that is reasonably practicable and to resume the performance of its obligations as soon as reasonably possible.

9. General Provisions

This Agreement supersedes all prior SLA agreements and communications between the parties relating to the subject matter herein. In the case of conflict, the terms of this Agreement shall prevail.

BullWall is free to change the terms of this Agreement at any time. BullWall shall use all reasonable endeavors and give the customer or 3rd party 60 days' notice in writing of any proposed change to the terms of this Agreement before they take effect.



Crown
Commercial
Service

Attachment 5 – Key Supplier Personnel and Key Sub-Contractors

- .8.1 The Parties agree that they will update this Attachment 5 periodically to record any changes to Key Supplier Personnel and/or any Key Sub-Contractors appointed by the Supplier after the Commencement Date for the purposes of the delivery of the Services.

Part A – Key Supplier Personnel

[Guidance Note: Insert details of Key Supplier Personnel, their Key Role(s) and Duration in the below table or delete the table in its entirety and insert Not Applicable if there is no Key Supplier Personnel]

| Key Supplier Personnel | Key Role(s) | Duration |
|--|--------------------|----------|
| David Blenkinsop Government Strategic Account Director Cyber Mobile: 07771 618494 david.blenkinsop@ricoh.co.uk | Account Management | 15 years |
| | | |
| | | |

Part B – Key Sub-Contractors

[Guidance Note: Insert details of Key Sub-Contractors and any additional information required in the below table or delete the table in its entirety and insert Not Applicable if there are no Key Sub-Contractors. This table should be based on the Key Sub-Contractors set out in Schedule 7 of the Framework]

N/a as Ricoh UK Limited are responsible for the delivery of the Services.

(Software in scope is Third Party COTS Software being procured and re-sold by Ricoh, but this aspect does not give rise to sub-contracting).



Crown
Commercial
Service

| Key Sub-contractor name and address (if not the same as the registered office) | Registered office and company number | Related product/Service description | Key Sub-contract price expressed as a percentage of total projected Charges over the Contract Period | Key role in delivery of the Services |
|--|--------------------------------------|-------------------------------------|--|--------------------------------------|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |



Crown
Commercial
Service

Attachment 6 – Software

- .8.1 The Software below is licensed to the Buyer in accordance with Clauses 20 (*Intellectual Property Rights*) and 21 (*Licences Granted by the Supplier*).
- .8.2 The Parties agree that they will update this Attachment 6 periodically to record any Supplier Software or Third Party Software subsequently licensed by the Supplier or third parties for the purposes of the delivery of the Services.

Part A – Supplier Software

The Supplier Software includes the following items:

| Software | Supplier (if an Affiliate of the Supplier) | Purpose | Number of Licences | Restrictions | Number of Copies | Type (COTS or Non-COTS) | Term/ Expiry |
|----------|--|---------|--------------------|--------------|------------------|-------------------------|--------------|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

Part B – Third Party Software



Crown
Commercial
Service

The Third-Party Software shall include the following items:

| Third Party Software | Supplier | Purpose | Number of Licences | Restrictions | Number of Copies | Type (COTS or Non-COTS) | Term/ Expiry |
|--|--------------|---------------------------|--------------------|--------------|------------------|-------------------------|-----------------------------|
| Bullwall Ransomware Containment - Cyber Security | Bullwall a/s | Ransomware Cyber Security | 4500 | N/a | 1 | Non-COTS | 18 months from commencement |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

Attachment 7 – Financial Distress

For the purpose of Schedule 7 (Financial Distress) of the Call-Off Terms, the following shall apply:

PART A – CREDIT RATING THRESHOLD

| Entity | Credit Rating (long term) <i>(insert credit rating issued for the entity at the Commencement Date)</i> | Credit Rating Threshold <i>(insert the actual rating (e.g. AA-) or the Credit Rating Level (e.g. Credit Rating Level 3))</i> |
|-------------------------------|---|---|
| Supplier | [Rating Agency 1] – [insert rating for Rating Agency 1] | [Rating Agency 1] – [insert threshold for Rating Agency 1] |
| | [Rating Agency 2] – [insert rating for Rating Agency 2] | [Rating Agency 2] – [insert threshold for Rating Agency 2] |
| | [etc.] | [etc.] |
| [Guarantor] | [Rating Agency 1] – [insert rating for Rating Agency 1] | [Rating Agency 1] – [insert threshold for Rating Agency 1] |
| | [Rating Agency 2] – [insert rating for Rating Agency 2] | [Rating Agency 2] – [insert threshold for Rating Agency 2] |
| | [etc.] | [etc.] |
| [Key Sub-contractor 1] | [etc.] | [etc.] |
| [Key Sub-contractor 2] | [etc.] | [etc.] |

PART B – RATING AGENCIES

- [Rating Agency 1 (e.g Standard and Poors)]
 - Credit Rating Level 1 = [AAA]
 - Credit Rating Level 2 = [AA+]
 - Credit Rating Level 3 = [AA]
 - Credit Rating Level 4 = [AA-]
 - Credit Rating Level 5 = [A+]
 - Credit Rating Level 6 = [A]
 - Credit Rating Level 7 = [A-]

- Credit Rating Level 8 = [BBB+]
- Credit Rating Level 9 = [BBB]
- Credit Rating Level 10 = [BBB-]
- Etc.
- [Rating Agency 2 (e.g Moodys)]
 - Credit Rating Level 1 = [Aaa]
 - Credit Rating Level 2 = [Aa1]
 - Credit Rating Level 3 = [Aa2]
 - Credit Rating Level 4 = [Aa3]
 - Credit Rating Level 5 = [A1]
 - Credit Rating Level 6 = [A2]
 - Credit Rating Level 7 = [A3]
 - Credit Rating Level 8 = [Baa1]
 - Credit Rating Level 9 = [Baa2]
 - Credit Rating Level 10 = [Baa3]
 - Etc.
- [Rating Agency 3 (etc.)]
 - Credit Rating Level 1 = [XXX]
 - Etc.
- Attachment 8 – Governance

PART A – SHORT FORM GOVERNANCE

For the purpose of Part A of Schedule 7 (Short Form Governance) of the Call-Off Terms, the following board shall apply:

| Operational Board | |
|--|------------------|
| Buyer Members for the Operational Board | [Not Applicable] |
| Supplier Members for the Operational Board | [Not Applicable] |
| Frequency of the Operational Board | [Not Applicable] |
| Location of the Operational Board | [Not Applicable] |

PART B – LONG FORM GOVERNANCE

For the purpose of Part B of Schedule 7 (Long Form Governance) of the Call-Off Terms, the following boards shall apply:

| SERVICE MANAGEMENT BOARD | |
|--|------------------|
| Buyer Members of Service Management Board (include details of chairperson) | [Not Applicable] |
| Supplier Members of Service Management Board | [Not Applicable] |
| Start Date for Service Management Board meetings | [Not Applicable] |
| Frequency of Service Management Board meetings | [Not Applicable] |
| Location of Service Management Board meetings | [Not Applicable] |

| Programme Board | |
|---|------------------|
| Buyer members of Programme Board (include details of chairperson) | [Not Applicable] |
| Supplier members of Programme Board | [Not Applicable] |
| Start date for Programme Board meetings | [Not Applicable] |
| Frequency of Programme Board meetings | [Not Applicable] |
| Location of Programme Board meetings | [Not Applicable] |

| Change Management Board | |
|---|------------------|
| Buyer Members of Change Management Board (include details of chairperson) | [Not Applicable] |
| Supplier Members of Change Management Board | [Not Applicable] |

| | |
|---|------------------|
| Start Date for Change Management Board meetings | [Not Applicable] |
| Frequency of Change Management Board meetings | [Not Applicable] |
| Location of Change Management Board meetings | [Not Applicable] |

| Technical Board | |
|---|------------------|
| Buyer Members of Technical Board (include details of chairperson) | [Not Applicable] |
| Supplier Members of Technical Board | [Not Applicable] |
| Start Date for Technical Board meetings | [Not Applicable] |
| Frequency of Technical Board meetings | [Not Applicable] |
| Location of Technical Board meetings | [Not Applicable] |

| Risk Management Board | |
|--|------------------|
| Buyer Members for Risk Management Board (include details of chairperson) | [Not Applicable] |
| Supplier Members for Risk Management Board | [Not Applicable] |
| Start Date for Risk Management Board meetings | [Not Applicable] |
| Frequency of Risk Management Board meetings | [Not Applicable] |
| Location of Risk Management Board meetings | [Not Applicable] |

Attachment 9 – Schedule of Processing, Personal Data and Data Subjects

This Attachment 9 shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Schedule shall be with the Buyer at its absolute discretion.

1.1.1.1 The contact details of the Buyer's Data Protection Officer are: **medwayft.dpo@nhs.net**

1.1.1.2 The contact details of the Supplier's Data Protection Officer are: **Ricoh does not have a designated Data Protection Officer (not required for our organisation under regulations/law). For data protection related notices please send to: Ricoh c/o Group Legal, 20 Triton Street, London NW1 3BF**

1.1.1.3 The Processor shall comply with any further written instructions with respect to processing by the Controller.

1.1.1.4 Any such further instructions shall be incorporated into this Attachment 9.

| Description | Details |
|--|--|
| Identity of Controller for each Category of Personal Data | <p>[The Authority is Controller and the Supplier is Processor</p> <p>The Parties acknowledge that in accordance with Clause 34.2 to 34.15 and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the following Personal Data:</p> <ul style="list-style-type: none"> Username, staff names, file names and system/infrastructure access attempts |
| Duration of the processing | Duration of stated contract period |
| Nature and purposes of the processing | Technical logs and information associated with usernames, access attempts and file details will be recorded and used within this system. This data is used to provide vulnerability protection against ransomware attacks and offer privileged access management tools to internal staff with elevated permissions and 3rd party support providers to provide additional assurance and protections against cyber threats. |
| Type of Personal Data | Username, details of access, file names. |
| Categories of Data Subject | Trust Staff usernames and file interactions, privileged account details (usernames) and activity, File names and activity (access and changes) |
| Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data | Data will be held for the duration of the contract. Medway NHS Foundation Trust's internal IT team will be responsible for the destruction of data held on local servers within the Trust's IT infrastructure. Data destruction certificates would be requested for any associated data held within supplier hosted infrastructure. |

Attachment 10 – Transparency Reports

| Title | Content | Format | Frequency |
|--------------------------|----------------|---------------|------------------|
| [Performance] | | | |
| [Charges] | | | |
| [Key Sub-Contractors] | | | |
| [Technical] | | | |
| [Performance management] | | | |










Medway NHS Foundation Trust to cover PO 250015795


Final Audit Report

2025-03-26


| | |
|-----------------|---|
| Created: | 2025-03-21 |
| By: | Maggie Sharp (maggie.sharp@ricoh.co.uk) |
| Status: | Signed |
| Transaction ID: | CBJCHBCAABAAg1MWRRefQb5C0ufY3g2zkHD7eqLjZBBmx |

"Medway NHS Foundation Trust to cover PO 250015795" History

-  Document created by Maggie Sharp (maggie.sharp@ricoh.co.uk)
2025-03-21 - 16:08:48 GMT - IP address: 165.225.196.90
-  Document emailed to simon.wombwell@nhs.net for signature
2025-03-21 - 16:12:57 GMT
-  Email viewed by simon.wombwell@nhs.net
2025-03-21 - 22:19:17 GMT - IP address: 146.75.174.12
-  Email viewed by simon.wombwell@nhs.net
2025-03-25 - 19:17:06 GMT - IP address: 194.73.125.107
-  Signer simon.wombwell@nhs.net entered name at signing as Simon Wombwell
2025-03-25 - 19:18:53 GMT - IP address: 194.73.125.107
-  Simon Wombwell (simon.wombwell@nhs.net) has agreed to the terms of use and to do business electronically with Ricoh UK Ltd
2025-03-25 - 19:18:55 GMT - IP address: 194.73.125.107
-  Document e-signed by Simon Wombwell (simon.wombwell@nhs.net)
Signature Date: 2025-03-25 - 19:18:55 GMT - Time Source: server - IP address: 194.73.125.107
-  Document emailed to marco.pezzani@ricoh.co.uk for signature
2025-03-25 - 19:18:57 GMT
-  Email viewed by marco.pezzani@ricoh.co.uk
2025-03-26 - 09:31:12 GMT - IP address: 104.47.11.254

 Signer marco.pezzani@ricoh.co.uk entered name at signing as Marco Pezzani

2025-03-26 - 09:31:54 GMT- IP address: 147.161.144.122

 Marco Pezzani (marco.pezzani@ricoh.co.uk) has agreed to the terms of use and to do business electronically with Ricoh UK Ltd

2025-03-26 - 09:31:56 GMT- IP address: 147.161.144.122

 Document e-signed by Marco Pezzani (marco.pezzani@ricoh.co.uk)

Signature Date: 2025-03-26 - 09:31:56 GMT - Time Source: server- IP address: 147.161.144.122

 Agreement completed.

2025-03-26 - 09:31:56 GMT