IWAREHOUSE TELEMATICS SYSTEM TERMS
(Australia)

These terms are an agreement between the Raymond-authorized reseller (the "**Reseller**") and customer (the "**Customer**") identified on the agreement between Reseller and Customer (the "**Underlying Agreement**") and govern Customer's rental and use of one or more units of the iWAREHOUSE® Telematics System (the "**iW Solution**") provided to Customer under the Underlying Agreement.

These terms were last updated on **May 1, 2023** and are effective as between Reseller and Customer as of the effective date of the Underlying Agreement.

The parties therefore agree as follows:

1. The iW Solution.

(a) Reseller shall provide the iW Solution to Customer on the pricing and other terms specified in the Underlying Agreement and this agreement. It is Customer's responsibility to ensure that it has the information systems (e.g., internet connectivity, network infrastructure) specified in the Documentation or otherwise reasonably necessary for Customer to use the iW Solution. Customer's noncompliance with the preceding sentence will not relieve Customer of its payment obligations hereunder.

(b) Software. Reseller hereby grants Customer a limited, non-exclusive, non-transferable license, without the right to sublicense, to use the Software solely as necessary for Customer to use the iW Solution for its own internal business purposes in Australia (the "**Permitted Purpose**"). "**Software**" means all computer programs, whether in object code, script or other form, provided by or on behalf of Reseller as a component of the iW Solution, including computer programs incorporated into or otherwise running on the Equipment ("**Embedded Software**"), subsequent minor changes, fixes or patches to a current version of Software ("**Updates**") and new versions of Software that replace a current version of Software and adds new features, functionality or enhancements beyond the minor changes found in an Update ("**Upgrades**"). Customer shall not, and shall not permit others to: (1) sell, lease, rent, timeshare or distribute the Software; (2) disassemble, decompile, reverse engineer or otherwise attempt to derive the Software's source code; (3) publish, provide or otherwise make available to any third party, any competitive, performance or benchmark tests or analysis relating to the Software; (4) remove, alter or obscure any proprietary notices thereon; (5) export the Software out of Australia; or (6) use any Embedded Software separately from the Equipment on which it is integrated, or for any purpose other than using and managing the Equipment on which the Embedded Software is installed. During the warranty period, as that period is identified in the Underlying Agreement, Customer shall receive, without charge, all commercially available Updates. Customer acknowledges that Updates might be installed without prior notice to Customer. Reseller may make Upgrades available, the use of which might be contingent upon Customer's agreement to additional terms or payment of additional fees.

(c) Documentation. Reseller hereby grants Customer a non-exclusive, non-transferable license, without the right to sub-license, to use any information, whether provided in written or electronic form, related to the use or functionality of the iW Solution that Reseller provides or otherwise makes available to Customer (the "**Documentation**") solely for the Permitted Purpose. Customer may make a reasonable number of copies of the Documentation for back-up or archival purposes only but shall not remove, alter or obscure any proprietary notices thereon.

(d) Equipment. Customer shall: (A) use the Equipment solely for the Permitted Purpose; (B) not, and shall not permit others to, disassemble or reverse engineer the Equipment or remove any proprietary notices thereon; (C) not re-sell the Equipment (any sales of Equipment by Customer are hereby void *ab initio*); (D) protect the Equipment with equal or better care than Customer protects similar types of equipment owned or controlled by Customer, but with no less than a reasonable degree of care; and (E) upon prior notice, permit Reseller and any of its authorized representatives to inspect the Equipment.

(e) Cloud Services.

(1) Reseller hereby grants Customer a non-exclusive, non-transferable right to enable any Customer employee or contractor (each, an "**Authorized User**") to access and use the online, web-based services made available to Customer in connection with the iW Solution (the "**Cloud Services**") solely for the Permitted Purpose. Customer shall ensure that each Authorized User uses the Cloud Services in compliance with this agreement and will remain liable to Reseller for any acts or omissions associated with an Authorized User account. Customer shall not, and shall ensure that Authorized Users do not: (A) remove, alter or obscure any copyright, trademark or other proprietary notices; (B) use or access any Cloud Service to provide service bureau, time-sharing or other services to third parties or make any Cloud Service available to third parties as a managed or network provisioned service; (C) reverse engineer, decompile, disassemble or otherwise attempt to derive any Cloud Service source code; (D) modify or create derivative works based on the Cloud Services; (E) attempt to undermine the security or integrity of the Cloud Services or attempt to gain unauthorized access to any Cloud Service; (F) attempt to view, access or copy any material or data other than that which Customer is authorized to access; (G) transmit, input or store any information or data into the Cloud Services that breaches any third party right (including any rights by copyright, trademark, trade secret or patent or any moral right or other intellectual or proprietary right recognized by any jurisdiction, whether now existing or hereafter arising (collectively, "**Intellectual Property**")); (H) attack, disrupt or perform a penetration test on any Cloud Service; or (I) access the Cloud Services in order to build a similar or competitive product. Customer shall use reasonable efforts to prevent and terminate unauthorized access to and use of any Cloud Service. Customer shall promptly notify Reseller of any known or reasonably suspected unauthorized use of, or access to, the Cloud Services.

(2) Customer acknowledges that Reseller may on one or more occasions, add, modify, discontinue or deprecate Cloud Service features or functionality. Reseller shall have the right to immediately suspend any portion of Customer's access to and use of the Cloud Services, including any Authorized User's account, if Reseller determines that its access to or use of the Cloud Services (A) is prohibited by law or this agreement; (B) poses a security threat to the Cloud Services, Reseller or any third party; or (C) may adversely impact the integrity of the Cloud Services or the content of any non-party. Reseller shall provide Customer with prior notice of such suspension; provided, however, if prior notice is not possible or is otherwise unreasonable,

Reseller shall notify Customer as soon as reasonably possible following such suspension. Any suspension hereunder will not excuse Customer's payment obligations.

(3) Reseller shall provide the Cloud Services to Customer in accordance with the terms set forth in exhibit 1 (the "**SLA**"). The service credits, as calculated in the SLA, are Customer's exclusive remedy and Reseller's sole liability for a breach of the preceding sentence.

(4) The iW Solution might include Customer access to the Raymond GATEWAY™ Cloud Service. The Raymond GATEWAY Cloud Service is in compliance with the security standards set forth in exhibit 2.

(f) Customer Content. Customer is solely responsible for the content and preservation of all data (i) manually inputted into the Cloud Services by Customer and its Authorized Users; or (ii) generated from Customer's use of the iW Solution and made available to Customer through the Cloud Services or Software. (collectively, "**Customer Content**"). Customer has and shall maintain the legal bases and right to share Customer Content with Reseller and its service providers. Customer shall secure and maintain all rights in Customer Content necessary for the provision of the Cloud Services without violating the rights of any non-party or otherwise obligating Reseller or its service providers. Reseller does not assume any obligations with respect to the Customer Content other than as expressly set forth in this agreement or as required by applicable law. Customer is responsible for providing any required notices to, and obtaining any required consents from, any relevant individuals (including employees of Customer), as needed, to permit Reseller to collect, use, store, and disclose such individuals' personal information (including Customer Content, to the extent that such data would constitute personal information) for the purposes of providing, evaluating and improving Reseller's and its licensors' products and services pursuant to this agreement. Such notices and consents shall conform to all applicable privacy and data protection laws, as well as any applicable guidance issued or published by relevant regulatory authorities and shall be subject to the review and approval of Reseller. Customer will retain evidence of such notices and consents and provide such evidence to Reseller promptly upon Reseller's request, including as needed for Reseller to respond to any claim or complaint by an individual, or any inquiry or investigation by any regulatory authority.

2. Intellectual Property.

(a) Reseller and its licensors and service providers are and shall remain the owner of all Intellectual Property rights in and to the iW Solution. The granting of access to any Cloud Service by Reseller should not be construed as granting or conferring any rights by license in the Cloud Services. Customer shall not, during the Term or at any time thereafter, attack the Intellectual Property rights of Reseller or its licensors or service providers in and to the iW Solution.

(b) Customer retains all Intellectual Property rights in and to the Customer Content. Customer hereby grants Reseller a worldwide, non-exclusive, paid-up, transferable, perpetual and irrevocable license for Reseller and its service providers and sub-processors to use, store, copy, transfer, modify, make available and communicate the Customer Content (1) as reasonably necessary to provide the iW Solution to Customer; (2) to improve and develop Raymond and Reseller products and services; and (3) to aggregate deidentified Customer Content with that of others to use for any business purpose during or after the Term, provided that Customer is not identifiable as the source of any such data.

3. Representations and Warranties.

(a) Each party represents and warrants to the other that it has the full power, capacity and authority to enter into and perform its obligations under this agreement and to make the grant of rights contained herein, and its performance hereunder does not violate or conflict with any other agreement to which it is a party.

(b) EXCEPT AS EXPRESSLY STATED IN THIS AGREEMENT OR THE UNDERLYING AGREEMENT, RESELLER MAKES NO OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR TITLE AND ALL SUCH WARRANTIES ARE HEREBY SPECIFICALLY DISCLAIMED. ANY EMPLOYEES, REPRESENTATIVES, AGENTS, OR DISTRIBUTORS OF RESELLER ARE NOT AUTHORIZED TO MODIFY OR MAKE ADDITIONS TO THIS WARRANTY THAT ARE BINDING ON RESELLER. ANY SUCH STATEMENTS, WHETHER WRITTEN OR ORAL, DO NOT CONSTITUTE ADDITIONAL WARRANTIES.

4. Confidentiality.

(a) "**Confidential Information**" means any information, whether oral or written, received by the Receiving Party from Disclosing Party that a reasonable person, given the nature and circumstances of disclosure, would know to be confidential; provided, however, Confidential Information does not include any information that is: (i) already public when the Disclosing Party discloses it to Receiving Party or becomes public (other than as a result of breach of this agreement by Receiving Party) after the Disclosing Party discloses it to the Receiving Party; (ii) lawfully obtained, after it is disclosed under this agreement, from a third-party who is not otherwise bound by a confidentiality agreement with Disclosing Party; (iii) already in the possession of the Receiving Party or any of its Representatives on a non-confidential basis prior to Disclosing Party's disclosure; (iv) independently developed by the Receiving Party without use or reference to the Disclosing Party's Confidential Information and without violating any obligation under this agreement; or (v) released without restriction by Disclosing Party.

(b) The party, its affiliates or agents that receives Confidential Information (the "**Receiving Party**") of the other party, its affiliates or agents (the "**Disclosing Party**") shall: (1) treat the Disclosing Party's Confidential Information as confidential; (2) use the same degree of care as it maintains the confidentiality of its own confidential information, but in no event will the Receiving Party use less than a reasonable degree of care to maintain the confidentiality of Disclosing Party's Confidential Information; (3) not use the Disclosing Party's Confidential Information for any purpose other than as expressly permitted by or in connection with its obligations under this agreement; and (4) prevent disclosure of the Disclosing Party's Confidential Information to third parties; provided,

however, disclosure may be made on a confidential basis to Receiving Party's parent, subsidiary and affiliate companies, and their officers, directors, employees and contract employees, agents, consultants, financing sources and advisors (collectively, "**Representatives**") who need to know in connection with this agreement, so long as the Representatives are aware of the confidential nature and are bound to preserve the Confidential Information's confidentiality. The Receiving Party shall be responsible for ensuring that its Representatives keep the Confidential Information confidential, do not disclose or divulge the same to any unauthorized person or entity and abide by the use restrictions contained herein. If either party or any of its Representatives loses or makes an unauthorized disclosure of the Confidential Information, it shall promptly notify the other party, provide a description of the circumstances of the loss or unauthorized disclosure and use reasonable efforts to retrieve the lost or wrongfully disclosed Confidential Information.

(c) Notwithstanding anything in this section 4 to the contrary, Customer Confidential Information does not include any feedback, suggestion or idea provided by Customer. Reseller and The Raymond Corporation ("**Raymond**") shall have the right to use, profit from, disclose, publish and otherwise exploit any feedback, suggestion or idea, without compensation to Customer. Customer hereby relinquishes and waives any Intellectual Property right it might have in any feedback, suggestion or idea.

(d) The Disclosing Party's Confidential Information, and all permitted copies, will remain the property of the Disclosing Party, and the Disclosing Party shall have the right to demand its return, in whole or in part, at any time, upon giving written notice to the Receiving Party. Upon receipt of such notice, the Receiving Party shall return the Confidential Information and all copies in its possession to the Disclosing Party as soon as is reasonably practical, but in no more than 30 days. Confidential Information incorporated in documents will be destroyed by Receiving Party. If the Receiving Party has destroyed any copies of Disclosing Party's Confidential Information, Receiving Party shall confirm the destruction in the letter accompanying the return of any documents or copies. Notwithstanding the foregoing sentences, (1) the Receiving Party shall not be obligated to return or destroy any Confidential Information the Receiving Party is retaining pursuant to a document retention hold established in connection with any civil or criminal investigation or litigation for the period the document retention hold is in effect, at which time the Confidential Information will be returned to the Disclosing Party or destroyed as aforesaid; and (2) to the extent Receiving Party's computer back-up procedures create copies of the Confidential Information, the Receiving Party may retain such copies in its archival or back-up computer storage for the period the Receiving Party normally archives backed-up computer records.

(e) The Receiving Party may disclose the Disclosing Party's Confidential Information that it is obligated, on the advice of legal counsel, to produce by law or under order of a court of competent jurisdiction or other similar requirement of a government agency, for the limited purpose required by the court or government agency, so long as the Receiving Party, to the extent legally permitted, provides the Disclosing Party with prompt written notice with sufficient time to permit the Disclosing Party to seek a protective order to protect its Confidential Information from disclosure.

(f) Each party recognizes that the Disclosing Party might have no adequate remedy at law if the Receiving Party does not comply with its obligations under this section 4. Therefore, a grant of injunctive relief would be appropriate to restrain any breach, threatened breach, or otherwise to specifically enforce any obligations of Receiving Party under this agreement.

(g) The requirements imposed by this section 4 will continue for three years following the termination or expiration of this agreement.

5. Indemnification.

(a) Reseller Indemnification. Reseller shall defend, indemnify, and hold harmless Customer and its officers, directors, employees and agents against all losses, damages, penalties, judgments, liabilities, settlements and expenses, including reasonable attorney fees and other expenses of litigation, settlement or defense (collectively, "**Indemnifiable Losses**") arising out of or resulting from any claim, suit, proceeding or cause of action brought by a non-affiliated third party (each, a "**Claim**") in connection with an allegation that Customer's use of the iW Solution infringes or misappropriates the Intellectual Property rights of any person. Notwithstanding the foregoing, Reseller shall have no defense or indemnity obligation for Claims arising from (1) Customer's use of the iW Solution not in compliance with this agreement, the Documentation or Reseller's reasonable instructions; (2) modification to any portion of the iW Solution not approved in writing or performed by Reseller or its agents (3) Reseller's or any of its representatives' conformance with specifications provided by Customer; (4) any use of the iW Solution in combination with other products, equipment, software or data not supplied by Reseller; or (5) Customer's failure to implement an update or enhancement provided by Reseller. If the iW Solution becomes, or is likely to become, the subject of Claim, then, in addition to defending the Claim and paying any damages as required in this section, Reseller may either replace or modify the iW Solution, providing not less than the functionalities specified in this agreement and the Underlying Agreement, to make them non-infringing or misappropriating; or procure for Customer the right to continue using the iW Solution. If Reseller determines that neither of the foregoing is feasible or otherwise reasonable, Reseller shall have the right to immediately terminate the Underlying Agreement and refund to Customer the prorated portion of any amounts paid thereunder. The remedies set forth in this section 7(a) will be Customer's sole remedy, and Reseller's sole liability, for any Claim.

(b) Customer Indemnification. Customer shall defend, indemnify and hold harmless Reseller, Raymond and the officers, directors, employees and agents of each against all Indemnifiable Losses arising out of or resulting from any Claim in connection with (1) Customer's or any of its contractor's, subcontractor's or agent's use of the iW Solution not in accordance with the Documentation, the Permitted Purpose, this agreement or in any unlawful manner; (2) the negligence or intentional misconduct of Customer or its employees, agents, servants, subcontractors or vendors; (3) any breach of alleged breach of this agreement by Customer; or (4) an allegation that any Customer Content infringes or misappropriates any Intellectual Property, privacy or other legal right of any third party.

(c) Procedure. A party (the "**Indemnified Party**") seeking indemnification or defense shall give prompt notice to the other party (the **"Indemnifying Party**") upon learning of any Claim. If the Indemnified Party does not promptly notify the Indemnifying Party of the Claim, the Indemnifying Party will be relieved of its indemnification and defense obligations with respect to the Claim to the extent the Indemnifying Party was prejudiced by that failure. The Indemnified Party shall allow the Indemnifying Party to control the defense and settlement of the indemnified Claim and shall reasonably cooperate with the Indemnifying Party. After the Indemnifying Party assumes the defense of the indemnified Claim, the Indemnified Party will bear the expenses of any

additional counsel retained by the Indemnified Party, and the Indemnifying Party will not be liable to such party under this agreement for any legal or other expenses subsequently incurred by such party. The Indemnifying Party shall use counsel reasonably experienced in the subject matter at issue and shall only settle a Claim without the written consent of the Indemnified Party if the settlement (1) does not entail any admission on the part of the Indemnified Party that it violated any law or infringed the rights of any person; (2) has no effect on any other claim against the Indemnified Party; (3) provides as the claimant's sole relief monetary damages that are paid in full by the Indemnifying Party; and (4) requires that the claimant releases the Indemnified Part from all liability alleged in the Claim.

6. **LIMITATION OF LIABILITY.** RESELLER WILL NOT BE LIABLE TO CUSTOMER FOR INDIRECT, INCIDENTAL, BUSINESS INTERRUPTION OR CONSEQUENTIAL DAMAGES, INCLUDING ANY LOSS OF REVENUE, PROFITS, SALES, DATA OR REPUTATION, WHETHER ARISING UNDER CONTRACT OR TORT AND REGARDLESS OF THE THEORY OF LIABILITY. THESE EXCLUSIONS APPLY EVEN IF IT HAS BEEN ADVISED OF THE POSSIBILITY OF THESE DAMAGES, AND EVEN IF ANY REMEDY FAILS OF ITS INITIAL PURPOSE. IN NO EVENT WILL THE CUMULATIVE LIABILITY OF RESELLER, TOGETHER WITH ITS SUPPLIERS, LICENSORS AND AFFILIATES, ARISING OUT OF OR RELATED TO THIS AGREEMENT OR THE ORDER, EXCEED THE TOTAL PAYMENTS RECEIVED BY RESELLER FROM CUSTOMER UNDER THE ORDER, WHETHER ARISING UNDER WARRANTY/GUARANTEE, CONTRACT, NEGLIGENCE, STRICT LIABILITY, INDEMNIFICATION, DEFENSE OR ANY OTHER CAUSE OR COMBINATION OF CAUSES.

7. **Third Party Beneficiary.** Raymond is an intended third party beneficiary of this agreement, and shall be entitled to directly enforce and rely upon, each provision of this agreement that confers a right or remedy in its favor.

8. **Assignability.** Except with Reseller's prior written consent, Customer shall not assign its interest in, or delegate any of its duties under, this agreement. Any unauthorized assignment or delegation will be null, void and of no force or effect and will constitute a material breach of this agreement.

9. **Governing Law.** The laws of the State of New York govern the validity, interpretation and performance of this agreement as well as all adversarial proceedings arising out of this agreement, without giving effect to any laws, rules or provisions that would cause application of the laws of any jurisdiction other than the State of New York. If either party brings against the other party any proceeding arising out of this agreement, that party shall bring that proceeding only in a state court located in Chenango County, New York or a federal court located in the Northern District of New York. The application of the United Nations Conventions on Contracts for the International Sale of Goods is excluded.

10. **Notice.** All notices, consents, communications or transmittals under this agreement will be in writing and will be deemed received on the day of delivery if personally hand delivered or sent by facsimile or electronic transmission (with written confirmation of the completed transmittal); or within two business days if mailed as certified or registered mail with return receipt, postage prepaid addressed to the party to whom notice is given at the address the party provided in the Underlying Agreement.

11. **Independent Contractors.** The parties are independent contractors only and are not partners, master/servant, principal/agent or involved herein as parties to any other similar legal relationship with respect to the transactions contemplated under this agreement or otherwise, and no fiduciary, trust, or advisor relationship, nor any other relationship imposing vicarious liability shall exist between the parties under this agreement or otherwise at law.

12. **Severability**. If a dispute between the parties arises out of this agreement or the subject matter of this agreement, the parties desire that the court interpret this agreement as follows: (a) with respect to any provision that the court holds to be unenforceable, by modifying that provision to the minimum extent necessary to make it enforceable or, if that modification is not permitted by law, by disregarding that provision; and (b) if an unenforceable provision is modified or disregarded in accordance with this section, by holding that the rest of the agreement will remain in effect as written; and (c) if modifying or disregarding the unenforceable provision would result in a failure of an essential purpose of this agreement, by holding the entire agreement unenforceable.

EXHIBIT 1

Service Levels

(a) The Cloud Services will achieve a monthly uptime percentage of at least 99.7% (the "**Service Level**"), where uptime is calculated as the total number of minutes in a calendar month minus the number of minutes of unavailability suffered in a calendar month, as such unavailability is limited in subsection (b), divided by the total number of minutes in the calendar month. If the Service Level is not met during any calendar month, then Customer, as its exclusive remedy, may, upon written request to Reseller in accordance with subsection (c) (a "**Service Level Claim**"), request a service credit calculated as follows:

Service Level	Service Credit
99.7% Cloud Service availability as averaged over a calendar month	5% monthly fees attributable to the Cloud Service during the affected calendar month

Upon approval of Customer's Service Level Claim, Reseller shall provide the service credit on a future amount owing from Customer. All Service Level Claims are subject to review and verification by Raymond. All service credits will be based on Raymond's or its sub-processor's measurement of its performance and will be final.

(b) A Cloud Service will not be considered unavailable, even if the Cloud Service is not actually accessible to an individual user or equipment, if such inaccessibility is due to: (1) Scheduled or emergency maintenance; (2) Customer's Internet or cellular connectivity; (3) Internet traffic outages, delays or problems not under Reseller's, Raymond's or Raymond's sub-processor's reasonable control; (4) Customer's failure to meet minimum hardware or software requirements set forth in this agreement or the iW Solution specifications; (5) hardware, software or services not provided by or on behalf of Reseller; (6) issues with Customer's network infrastructure; (7) Denial of Service ("**DoS**") or Distributed DoS attacks; or (8) any acts or omissions of the Customer, its representatives, contractors or subcontractors, other than the acts or omissions of Reseller or its representatives, or any use or user of the service authorized thereby.

(c) Customer shall submit all Service Level Claims within 30 days of the end of the month during which Reseller did not meet the Service Level and provide the following information:

(1) Customer name and locations affected;
(2) Name, email address and telephone number of a Customer designated contact; and
(3) Date, time and description of the downtime.

EXHIBIT 2

Raymond GATEWAY Cloud Service Security Standards

1. Service-Level Security.

(a) At the service level, Raymond uses a defense-in-depth strategy that protects data through multiple layers of security (physical, logical and data). A defense-in-depth strategy ensures that security controls are present at various layers of the service and that, should any one area fail, there are compensating controls. The strategy also includes tactics to detect, prevent, and mitigate security breaches. This involves regular improvements to service-level security features, including, but not limited to:

(1) Port scanning and remediation
(2) Perimeter vulnerability scanning
(3) Operating system security patching
(4) Network-level distributed denial-of-service (DDoS) detection and prevention

(b) Preventing breaches involves deleting unnecessary accounts when an employee leaves, changes groups, or does not use the account prior to its expiration. When commercially reasonable, human intervention is replaced by an automated, tool-based process.

(c) Raymond continues to invest in systems automation that helps identify abnormal and suspicious behavior and respond quickly to mitigate security risk. Raymond is also evolving an effective system of patch deployment that generates and deploys solutions to problems identified by the monitoring systems. Raymond conducts penetration tests to enable regular improvement of incident response procedures. These internal tests help Raymond security experts create a methodical, repeatable, and optimized response process and automation.

2. Physical Layer – Facility. Raymond's datacenter has redundant power lines with redundant UPSs, generators, environmental systems, redundant, diverse network connections, online and offsite daily backups of data and a fully configured disaster recovery site with 48 hour RPO and 48 hour recovery time objective (RTO) timeframes. Datacenter access is restricted 24 hours a day by job function—with access given to essential personnel. Physical access control uses multiple authentication and security processes, including badges, on-premises security officers, and continuous video surveillance. The datacenters are monitored using motion sensors, video surveillance, and security breach alarms. In case of a natural disaster, security also includes automated fire prevention and extinguishing systems. Raymond's obsolete storage media disposal process for hard drives and tape media leaving Raymond facilities is accomplished by physically drilling the media onsite. This goes beyond the "purge" requirement for these types of media defined by the NIST SP 800-88 document. For hard drives that are going to be repurposed, Raymond purges that media using over three passes of random overwrites, which conforms to the DoD 5220.22-M wipe standard.

3. Physical Layer – Network. Perimeter protection is implemented through the use of controlled devices at the network edge and on points throughout the network. The overarching principle of Raymond's network security is to allow only connections and communications that are necessary to allow systems to operate, blocking other ports, protocols and connections. Access control lists (ACLs) implemented in the form of tiered ACLs on routers, firewall rules and host based firewall rules are implemented in the network with restrictions on network communication, protocols, and port numbers. Raymond uses edge router security for monitoring at the network layer. Networks within Raymond's datacenter are further segmented to provide physical separation of critical back-end servers and storage devices from the public-facing interfaces. Raymond retains system logs for auditing and review.

4. Logical Layer. The logical layer of security involves many controls and processes implemented to secure the host machines, applications running on those hosts and from administrators that may perform any work on those host machines and applications.

5. Anti-malware, Patching, and Configuration Management. The use of anti-malware software is a principal mechanism for protection of Customer assets from malicious software. The software detects and prevents the introduction of computer viruses and worms into the systems. Anti-malware software provides both preventive and detective control over malicious software. Changes, such as updates, hotfixes, and patches made to the production environment, follow the same standard change management process. Patches are implemented within the time frame specified by the issuing company. Changes are both reviewed and evaluated by Raymond teams for applicability, risk, and resource assignment prior to being implemented.

6. Protection from Security Threats.

(a) Threat management strategy is a composite of identifying a potential threats intent, capability, and probability of successful exploitation of a vulnerability. The controls used to safe guard against such exploitations are founded upon industry-accepted security standards. The overall cyber threat landscape has evolved from traditional opportunistic threats to also include persistent and determined adversaries. Raymond provides Security Awareness training to all Raymond employees to address the evolving technical and non-technical security threats. Training provides current and relevant content for key threats such as phishing, use of privileged access and social engineering. This training is conducted annually and is mandatory for all Raymond employees.

(b) Raymond regularly improves its built-in security features. These include port scanning and remediation, perimeter vulnerability scanning, operating system patches, DDoS detection and prevention and live site penetration testing.

(c) Raymond's system and security alerts are harvested and correlated via an internal analysis system. The signals analyze alerts that are internal to the system as well as external signals.

(d) Raymond maintains a diligent incident response process, standard operating procedures in case of an incident, ability to deny or stop access to sensitive data and identification tools to promptly identify involved parties helps ensure that the mitigation is successful.

7. **Advanced Threat Protection**. Raymond employs an email filtering service that provides additional protection against specific types of advanced threats and a robust and layered anti-virus protection powered with three different engines against known malware and viruses.

8. **Verification**. Raymond has operationalized security into a process that can quickly adapt to security trends and industry-specific needs. Raymond engages in regular risk management reviews, and it develops and maintains a security control framework that meets the latest standards. Internal reviews are performed on a regular basis. Businesses today need productivity services that help users get more done while maintaining security in the face of ever-evolving threats. Raymond's platform incorporates security at every level, from application development to physical datacenters to end-user access.