Managed Endpoint Detection and Response (EDR) Services Agreement

This Managed Endpoint Detection and Response (EDR) Services Agreement (“Agreement”) governs the provision of managed EDR services delivered by KDDI America, Inc. (“Provider”) using CrowdStrike Falcon Complete and related technologies.

This Agreement applies to any individual or entity (“Customer”) that submits an Application for Service to Provider.

By submitting an Application for Service, Customer acknowledges and agrees to be bound by the terms and conditions set forth in this Agreement.

---

1. Service Authorization and Agreement Acceptance

Submission of an Application for Service constitutes Customer’s full and binding acceptance of this Agreement.

In the event of any inconsistency or conflict between the terms of the Application for Service and the provisions of this Agreement, the terms of this Agreement shall control and prevail.

---

2. Definitions

Party: Either the Customer or the Service Provider individually, and "Parties" means the Customer and the Service Provider collectively.

Customer: The entity receiving the Services under this Agreement.

Service Provider: The entity providing the Managed EDR Services under this Agreement.

CrowdStrike Falcon Platform: The suite of security technologies provided by CrowdStrike, including but not limited to the Falcon Sensor, Falcon Console, and associated cloud services.

Endpoint: Any customer-owned or -operated device, including desktop, laptops, servers, and supported virtual instances, on which the Falcon Sensor is deployed and actively reporting to the Falcon Platform.

EDR (Endpoint Detection and Response): Security functionality focused on monitoring, detecting, investigating, and responding to malicious activity or suspicious behavior on Endpoints.

Detection: An event, notification, or indicator generated by the Falcon Platform that requires review and may or may not be determined to be an Incident.

Incident: A security event or series of related events determined by Falcon Complete to indicate a confirmed compromise or malicious activity requiring investigation, containment, and/or remediation.

Containment: Response actions executed by the Service Provider to restrict, limit or isolate malicious activity, including but not limited to network isolation of an Endpoint, process termination, or blocking of persistence mechanisms.

Remediation: Actions taken following Containment to restore normal Endpoint functionality, including but not limited to malware removal, registry cleanup, configuration corrections, and other measures to eliminate the threat.

Customer Data: All data, logs, telemetry, detections, incident records, reports, and other information generated from Customer Endpoint or provided by Customer in connection with the Services.

Data Ownership: All rights, title, and interest in and to Customer Data shall remain solely with the Customer. The service Provider and/or CrowdStrike may process, store, and analyze Customer Data solely for the purpose of delivering the Services under this Agreement. Except as required by law, neither party shall transfer or disclose Customer Data to third parties without the Customer's prior written consent.

False Positive: A detection that is investigated and determined not to represent malicious or unauthorized activity.

Service Level Objective (SLO): Performance level target.

Services: The Managed EDR services provided under this Agreement, including monitoring, detection, containment, remediation, reporting, and incident response support, as further described in the Scope of Services.

Confidential Information: All non-public business, technical, financial, or security-related information disclosed by either Party in connection with this Agreement, whether in oral, written, electronic, or any other form, which is designated as confidential or which reasonably should be understand to be confidential given the nature of the information and the circumstances of disclosure.

Effective Date: The calendar date on which the Application for Service is signed by the customer. This date marks the official commencement of the agreement and serves as the starting point for any obligations, rights, or services outlined in the application.

---

3. Scope of Services

Provider shall deliver managed EDR services, including:

- Endpoint protection
- Extended detection and response
- Threat hunting
- 24/7 alert monitoring, containment, and remediation

Additional Scope Details:

- The Customer is responsible for installing the EDR agent on all applicable endpoints.
- Initial configuration of the dashboard and detection policies will be performed by the provider using recommended default settings.
- Any subsequent changes to dashboard settings must be made by the Customer.

Service Exclusions: The Services provided herein expressly exclude: (i) management, maintenance, or recovery of Customer backups; (ii) remediation of underlying software or system vulnerabilities; (iii) physical security of Endpoints; (iv) on-site support or hardware repair/replacement; and (v) resolution of issues caused by Customer's network configuration, third-party software not managed by Provider, or Customer's failure to adhere to its responsibilities under this Agreement. (vi) Detections triggered by policy rule matches.
(vii) Any services, tasks or activities other than those specifically noted in this Service Description.

---

4. Roles and Responsibilities

4.1 Provider Responsibilities Provider shall:

- Supply deployment documentation and onboarding guidance
- Monitor endpoint activity and initiate containment as needed
- Escalate alerts and incidents to Customer and/or Third-party partner
- Respond to active threats with remediation measures
- Maintain configuration and policy compliance
- Track license allocation and warranty eligibility

4.2 Customer Responsibilities Customer shall:

- Deploy Sensor agents on endpoints using provided instructions
- Ensure network/system access for telemetry collection
- Remove conflicting antivirus software prior to deployment
- Designate personnel for incident coordination
- Cooperate in investigation and remediation efforts
- Maintain endpoint hygiene and access control policies
- Cooperate with and follow the instructions given by Service Provider
- Provide the list of Customer authorized contacts and ensure it remains current.
- Accept all updates and upgrades to the Endpoint Agent necessary for the proper function and security of the Service.

Note: Sensor deployment is solely the Customer's responsibility unless otherwise agreed in writing.

---

5. Customer Representations and Warranties

Customer represents and warrants that: (i) it has the full legal right and authority to enter into this Agreement; (ii) it owns or has obtained all necessary rights and permissions to authorize Provider to perform the Services on the designated Endpoints; and (iii) its use of the Services will comply with all applicable laws.

---

6. Term, Renewal, and Termination

The minimum service term is twelve (12) months from the commencement date. This Agreement shall automatically renew for successive twelve (12) month periods unless either party provides written notice of non-renewal at least sixty (60) days prior to the end of the then-current term. Either party may terminate this Agreement for cause if the other party materially breaches this Agreement and fails to cure such breach within thirty (30) days of receiving written notice. Upon termination or expiration, Customer shall pay all outstanding fees incurred up to the effective date of termination, and each party shall, upon request, return or destroy the other's Confidential Information.

---

7. Service Level Objectives

Service Level Objectives (SLOs): These are performance targets and do not constitute enforceable guarantees:

- **Incident Notification:** Notify Customer of confirmed security incidents within one hundred and eighty (180) minutes of log analysis.
- **Inquiry Response Time:** Respond to Customer inquiries related to detections or incidents within one (1) business day.
- **Onboarding Completion:** Complete onboarding and configuration within ten (10) business days of the Effective Date.

Provider's obligation to meet the SLOs is expressly contingent upon Customer’s timely and complete fulfillment of its responsibilities as set forth in Section 4.2. Delays or failures by Customer to perform its obligations may relieve Provider of its SLO commitments.

Service Level Agreement (SLA): Not applicable.

---

8. Support and Communication

- Support is available 24 hours a day, 7 days a week, 365 days a year (24/7/365).
- In the event of a detection or incident, the provider’s Network Operation Center will initiate contact with the Customer if necessary
- Notifications will be delivered via ticketing system (ServiceNow) and / or by e-mail.
- Customer may contact the provider regarding detections or incidents via the ticketing system.

---

9. Language Support

- Support is available in Japanese and English.
- Note: Notifications regarding detections or incidents will be provided in English only.

---

10. Fees and Payment Terms

10.1 Service Fees Customer agrees to pay Provider the fees outlined in Application for the services described herein. Fees are based on:

- Number of protected endpoints
- Selected modules and add-ons
- Term length and renewal options

10.2 Payment Schedule Unless otherwise agreed:

- Fees are billed annually in advance.
- Payment is due within thirty (30) days of invoice date.

- Late payments may incur interest at 1.5% per month or the maximum allowed by law.

10.3 Adjustments Provider reserves the right to adjust fees upon renewal or in response to:

- Changes in endpoint volume
- Addition of new modules or services
- Modifications to CrowdStrike licensing terms

10.4 Taxes Customer shall be responsible for all applicable taxes, duties, or levies, excluding Provider's income taxes.

10.5 Provider Audit Rights Provider reserves the right, with reasonable prior notice to Customer and during normal business hours, to remotely audit the number of Endpoints on which the Sensor is deployed to ensure compliance with the terms of this Agreement and for billing verification purposes.

---

11. Change Management Process

Customer may request changes to the Services (e.g., increasing endpoint count or adding modules) via a written change order submitted to the Provider. The provider will evaluate the request and provide a quote for any associated fee adjustments. All change orders must be mutually agreed upon in writing by authorized representatives of both parties before implementation.

---

12. Risk of Loss

Provider is not responsible for service interruptions or damage caused by:

- Natural disasters, fire, or civil unrest
- Unauthorized modifications or misuse
- Third-party software conflicts or hardware failures

---

13. Limitation of Liability

To the maximum extent permitted by law, Provider shall not be liable for any indirect, incidental, special, consequential, or punitive damages, including but not limited to loss of profits, revenue, data, or business interruption, even if advised of the possibility of such damages.

Provider's total cumulative liability for any and all claims arising out of or relating to this Agreement and the herein referenced services shall be strictly limited to the total fees actually paid by Customer to Provider for the applicable services during the twelve (12) months immediately preceding the event giving rise to the claim.

This limitation of liability applies regardless of the legal theory asserted, including contract, tort, negligence, strict liability, or otherwise, and shall survive termination of this Agreement.

Customer shall, at its own expense, procure and maintain cyber liability insurance with coverage limits appropriate for its business risk.

---

14. Force Majeure

Neither party shall be liable for delays or failures caused by events beyond their reasonable control (Force Majeure). The parties' obligations under this Agreement shall resume once the Force Majeure disruption(s) ends.

---

15. Delivery and Installation

Deployment schedules shall be mutually agreed upon. Provider shall notify Customer of any anticipated delays. Sensor installation shall be performed by Customer in accordance with Section 4.2, unless otherwise specified in writing.

---

16. Warranty and Compliance

Provider disclaims all and all statutory warranties and warranties not expressly stated in this Agreement. Provider shall not engage in any unlawful activities and shall not be responsible for any errors, failures, or damages originating from the Customer’s systems, actions, or omissions, regardless of cause.

---

17. Data Ownership

All telemetry, alerts, and logs from Customer endpoints remain Customer property. Provider may use anonymized data for internal diagnostics and service improvement.

---

18. Indemnification

18.1 Customer Indemnification. Customer shall indemnify, defend, and hold harmless Provider and its affiliates, officers, directors, employees, and agents from and against any and all claims, damages, liabilities, costs, and expenses (including reasonable attorneys' fees) arising out of or related to (i) Customer's use of the Services in violation of applicable laws or third-party rights, or (ii) Customer's breach of this Agreement.

18.2 Provider Indemnification. Provider shall indemnify, defend, and hold harmless Customer from and against any third-party claims alleging that the Services, as provided by Provider and excluding any third-party technologies like CrowdStrike, directly infringe a third-party's U.S. patent or copyright. Provider's indemnification obligation is contingent upon Customer providing Provider with prompt written notice of the claim and reasonable cooperation in the defense of such claim. This section states Provider's sole liability and Customer's exclusive remedy for any infringement claim.

Limitation of Provider's liability is set forth in Section 13 and applies to all claims under this Agreement, including those arising from indemnification obligations.

---

19. Compliance

Provider shall comply with applicable laws and standards (e.g., GDPR, HIPAA, PCI-DSS) as applicable. Customer must disclose industry-specific requirements prior to onboarding.

---

20. Intellectual Property

CrowdStrike retains all rights, title, and interest in and to its technologies, including but not limited to Falcon Prevent, Insight XDR, and OverWatch.

Customer receives a limited, non-transferable, non-exclusive license to use these technologies solely for internal business purposes in accordance with this Agreement and applicable CrowdStrike licensing terms, as noted in Section 25 below.

Customer shall not reverse-engineer, decompile, disassemble, modify, copy, distribute, resell, or create derivative works of any CrowdStrike technologies or components thereof.

---

21. Confidentiality

Both parties shall protect the other party's confidential information and return or destroy it upon request of the disclosing party. The herein noted obligations shall apply during the term of the referenced services and shall survive for three (3) years after the termination and/or expiration of this Agreement or the referenced services. Exceptions apply to public or legally required disclosures.

---

22. Governing Law and Dispute Resolution

This Agreement shall be governed by the laws of the State of New York, without reference to its provisions on conflicts of law.

Prior to initiating arbitration, the aggrieved party shall notify the other party in writing of the dispute. The parties agree that their respective senior management will meet within thirty (30) days of such notice to attempt to resolve the dispute in good faith. If the dispute is not resolved within sixty (60) days of the initial notice, either party may then proceed to arbitration as described herein.

Disputes shall be resolved via binding arbitration administered by the American Arbitration Association (AAA) in New York, NY. All awards shall be limited to compensatory damages.

---

23. Notices

Notices shall be delivered via certified mail, email, or courier to the addresses listed above. Notices are deemed received upon actual receipt.

---

24. Waiver

Failure to enforce any provision shall not constitute a waiver of future rights.

---

25. Third-Party Licensing Terms

Customer agrees to comply with all applicable CrowdStrike licensing and warranty terms, including:

- CrowdStrike Terms & Conditions :

  https://www.crowdstrike.com/en-us/legal/terms-conditions/

- CrowdStrike Software Terms of Use :

https://www.crowdstrike.com/en-us/legal/software-terms-of-use/

Restrictions on reverse-engineering, resale, or modification of Falcon technologies are set forth in Section 20 of this Agreement and in CrowdStrike's licensing terms.

26. Entire Agreement

This Agreement, including all appendices (if applicable), constitutes the entire understanding between the parties and supersedes all prior agreements. Any amendments to this Agreement must be in writing and signed by both parties.