Mutual Non-Disclosure Agreement

Confidentiality for customer security assessments

Version 1.1 | 7 October 2026

This NDA takes effect when completed and signed by authorised representatives of both parties. It protects confidential information exchanged for the assessment described below.

Agreement particulars

Particular	Details
Disqnect	Disqnect AS, organisation number 936 620 744, Olaf Helsets vei 5, 0694 Oslo, Norway
Other party	**[legal name, registration number and registered address]**
Purpose	Scoping and preparing an authorised security assessment and, where separately contracted, conducting the assessment, reporting findings, supporting remediation and verifying fixes. Project or engagement: **[To be completed for the engagement]**
Effective date	Date of the last signature below
Related service agreements and processing/retention schedules	**[document references and versions, or "None - pre-contract discussions only"]**
Earlier disclosures covered	**[date and subject matter, or "None"]**
Disqnect agreement contact	privacy@disqnect.com
Disqnect security incident contact	security@disqnect.com
Other party agreement and security contacts	**[names or functions and email addresses]**

Each party may disclose or receive information. In relation to a particular disclosure, they are the **Disclosing Party** and the **Receiving Party** respectively.

1. Confidential information

1.1 **Confidential Information** means non-public information disclosed or made accessible for the Purpose that is marked confidential or that a reasonable recipient would understand to be confidential from its nature or the circumstances. It includes written, electronic, visual and oral information, demonstrations and information observed during an authorised engagement. Protection does not depend on a confidentiality label or a later written summary.

1.2 This includes security findings, vulnerabilities, reports, assessment evidence, credentials, network and system details, incident information, business plans, pricing, procurement discussions and non-public technical information about Disqnect Intelligence, software or devices. Copies, extracts and analyses that reveal such information are also protected. Information about a customer's systems obtained or recorded during testing is protected even when Disqnect creates the report or record.

1.3 Information lawfully shared on behalf of a customer, affiliate or another third party is protected on the same basis. Disclosure under this Agreement does not remove any applicable third-party rights or restrictions.

2. Permitted use and protection

2.1 The Receiving Party shall use Confidential Information only for the Purpose and shall disclose it only as permitted by this Agreement. It shall apply reasonable safeguards appropriate to the sensitivity of the information and at least the care it uses for its own similarly sensitive information.

2.2 Access shall be limited to personnel, professional advisers, auditors and contractors who need the information for the Purpose and are bound by contractual or professional confidentiality duties at least as protective as the relevant obligations here. The Receiving Party remains responsible for their handling of the information. Service providers may process Confidential Information only as necessary for the Purpose, under binding confidentiality and appropriate security obligations. For a separately contracted assessment, the parties shall identify authorised operational recipients, processing purposes, locations and applicable restrictions in an agreed processing schedule. That schedule applies to assessment Confidential Information whether or not it contains personal data. Provider changes follow the change and objection procedure agreed in that schedule or the related service agreement, together with any applicable DPA requirements. Publication of a provider list does not itself constitute authorisation.

2.3 Particularly sensitive material, including credentials and vulnerability evidence, shall be shared using appropriately protected channels and restricted access. Each party shall avoid unnecessary copies and shall not place the other party's Confidential Information in public repositories, public communications or personal accounts.

2.4 Confidential Information shall not be used to train or fine-tune models, or for the Receiving Party's independent product development or evaluation, without separate written permission from the Disclosing Party. Submission to an AI service requires written authorisation identifying the permitted purpose and recipient. For separately contracted assessments, the agreed processing schedule under clause 2.2 may authorise operational model inference necessary to deliver the assessment, reporting, remediation support and verification. That operational authorisation does not authorise independent product development or evaluation, model training or fine-tuning. Those uses require separate written permission specifying the purpose, permitted information, recipients and retention. A provider's no-training setting does not itself give that authorisation. A valid authorisation under another agreement does not release the Receiving Party from confidentiality obligations.

2.5 Neither party may publish the other party's non-public findings, name or logo as a customer reference, testimonial or case study without prior written permission. This does not restrict lawful disclosures under clause 4.

3. Exclusions

The Receiving Party may establish, through reliable records or other evidence, that information:

- was already lawfully known to it without a confidentiality restriction before disclosure;
- became publicly available without a breach of this Agreement or another confidentiality duty;
- was lawfully received from a third party entitled to disclose it without restriction; or
- was independently developed without use of the Confidential Information.

Only the information meeting an exclusion is exempt. Public availability of individual elements does not automatically make a non-public combination, customer context or assessment record public. Remembering information does not grant a separate right to use or disclose it.

4. Required and protected disclosures

4.1 Nothing in this Agreement prevents disclosure required by applicable law, a competent court or authority, or a legally protected report to an appropriate authority. It does not restrict lawful whistleblowing, regulatory cooperation or exercise of non-waivable statutory rights.

4.2 Where lawful and reasonably practicable, the Receiving Party shall notify the Disclosing Party before a required disclosure, provide an opportunity to seek protection, disclose only what is required and request confidential handling where available. Notice or consultation shall not delay compliance with a binding legal deadline or obstruct a protected report.

4.3 A public-sector party remains responsible for its obligations under applicable public-access, procurement and archives law. This Agreement does not determine whether a record is exempt from disclosure. Where lawful and practicable, the parties shall cooperate to identify protected information and appropriate redactions.

5. Unauthorised access or disclosure

The Receiving Party shall notify the Disclosing Party without undue delay after becoming aware of unauthorised access, use or disclosure affecting its Confidential Information. It shall take reasonable steps to contain the incident, preserve relevant evidence, mitigate harm and cooperate in remediation. Notice shall use the security contact in the particulars, include available relevant information and be supplemented as further material facts become known. Any shorter or more specific notification obligation in an applicable DPA or service agreement also applies.

6. Return, deletion and retained copies

6.1 On written request or when the Purpose ends, the Receiving Party shall cease unnecessary use and, at the Disclosing Party's choice, return or securely delete Confidential Information under its control, including unnecessary working copies and copies held by its representatives. Unless the service-record exception below applies, it shall complete this within 30 calendar days.

For assessment records covered by an agreed service retention, export and deletion schedule, that schedule governs during the services and on their termination, whether or not the records contain personal data. Other Confidential Information remains subject to the 30-calendar-day requirement above. Return does not authorise

continued use or retention of remaining copies. Nothing in this clause postpones an earlier deletion obligation imposed by applicable law, the applicable DPA or an agreed customer instruction. The restricted retention exceptions in clauses 6.2 and 6.3 remain subject to those requirements.

6.2 The Receiving Party may retain only the minimum information required by law or reasonably necessary to establish, exercise or defend legal claims. Such copies shall have restricted access, shall not be used for other purposes, and shall be deleted when the retention ground ends. Public-sector statutory archival duties remain applicable.

6.3 Residual copies in routine backups may remain until expiry under the documented backup schedule, for no longer than 90 days after active-copy deletion unless applicable law requires longer or the parties expressly agree another period in writing. Retained copies remain protected, shall not be restored for ordinary use, and shall be deleted again if restored for recovery. A stricter agreed DPA or service schedule takes precedence.

6.4 On request, the Receiving Party shall confirm completion and identify the categories of any retained copies, the retention grounds and applicable expiry periods. Continued confidentiality does not itself authorise continued retention.

7. Duration

7.1 This Agreement covers disclosures for the Purpose during the three years following the Effective Date and throughout any related contracted services continuing beyond that period, including their agreed return, deletion and closeout activities. It also covers earlier disclosures expressly identified in the particulars. Either party may end coverage of new pre-contract disclosures by giving 30 days' written notice. Such notice does not end coverage of disclosures for continuing contracted services or their closeout. The disclosure period ends when coverage for both pre-contract and contracted-service disclosures has ended. Neither expiry nor termination releases obligations relating to information already received.

7.2 Confidentiality and purpose restrictions continue for five years after the disclosure period ends. For information qualifying as a trade secret, they continue for as long as it retains that status. Non-public credentials and vulnerability or system-access information remain protected for as long as disclosure could reasonably compromise the relevant systems. Applicable statutory protection of personal data continues independently. The exclusions in clause 3 continue to apply.

8. Other agreements and rights

8.1 This Agreement protects confidentiality. It does not authorise security testing, grant system access, appoint a data processor or authorise an international data transfer. Scope and rules of engagement, service terms and any required DPA must be agreed separately. Neither party is obliged to disclose information or enter into a transaction.

8.2 No intellectual-property ownership is transferred, and no licence is granted beyond the limited use necessary for the Purpose. Ownership and permitted use of service deliverables are governed by the service agreement. This Agreement contains no exclusivity, non-compete or non-solicitation obligation.

8.3 The parties shall comply with both this Agreement and other applicable agreements. An applicable DPA governs personal-data processing and is not reduced by this NDA. The agreed operational processing and retention schedules govern the matters expressly assigned to them in clauses 2.2, 2.4 and 6.1; they do not otherwise reduce the confidentiality and purpose restrictions in this Agreement. A later agreement replaces or varies this NDA only where it expressly identifies that effect. Mandatory law prevails.

8.4 A party may seek damages and interim or other relief available under applicable law. This Agreement sets no predetermined penalty or liability cap. Any limitation in another agreement applies to this NDA only if that agreement expressly so provides. No remedy is automatic; the applicable legal requirements remain controlling.

9. Law, notices and signature

9.1 Norwegian law governs this Agreement. The parties shall seek to resolve disputes through their designated contacts. Oslo District Court (Oslo tingrett) is the agreed court of first instance, subject to mandatory jurisdiction rules. Either party may seek urgent protective relief from another competent court where necessary.

9.2 Written notices and permissions may be sent to the designated email contacts. Each party shall keep its contact details current. Permissions to expand a purpose or authorise additional uses must come from a representative authorised to give that permission; listing a security contact does not by itself grant that authority. Amendments must be agreed in writing by authorised representatives. If a provision is unenforceable, the remaining provisions continue to apply to the extent permitted by law.

9.3 The parties may sign electronically and in counterparts. Each signatory confirms authority to bind the named party. Accessing or downloading this template does not execute it.

Signatures

For Disqnect AS	**For the other party**
Name: **[To be completed for the engagement]**	Legal entity: **[To be completed for the engagement]**
Title: **[To be completed for the engagement]**	Name and title: **[To be completed for the engagement]**
Signature: _____	Signature: _____
Date: _____	Date: _____