XPScerpto Contributor Security Agreement

Document class: Contributor Agreement
Agreement ID: `SECURITY_POLICY`
Agreement version: `002`
Effective date: `2026-08-21`
Governing language: English
Lifecycle status: `ACTIVE`

Legal Identity, Governing Language, and Applicable Law

For this Agreement, **“XPScerpto”** means the XPScerpto platform currently operated by **Malek Dumaini**. The legal party operating XPScerpto for this Agreement is **Malek Dumaini, operating the XPScerpto platform**. Use of the XPScerpto name in this Agreement identifies the platform and does not represent that XPScerpto is a company or other legal entity.

English is the governing language of this Agreement. A translation may be provided for accessibility or convenience, but it does not replace or modify the English version. Mandatory protections under applicable law remain unaffected.

This Agreement is governed by the laws of the Federal Republic of Germany. It does not establish an exclusive forum. Jurisdiction is determined by the courts competent under applicable German and European Union law, including mandatory protective rules that cannot be excluded by agreement.

The legal operator’s replacement by a company or another person requires a documented material-change review and, where the legal text or party changes, a new Agreement version. Historical versions, hashes, acceptances, and

receipts remain associated with the legal operator and text that applied when they were created.

Editorial state: Editorial canonical candidate - not activated
Agreement lifecycle status: Not assigned. This candidate is not eligible for acceptance.

The Contributor enters into this Agreement with XPScerpto, the contracting party identified above. Within this Agreement, “XPScerpto” identifies the brand, platform, services, product, or controlled contribution process relevant to the provision. XPScerpto remains the named contracting party.

Only the English canonical text has governing legal effect. Any translation is supplied for access or convenience and cannot revise or supersede the English text. Mandatory applicable law continues to apply.

Section 4 contains the document-specific definitions. **MUST** imposes a binding obligation, **MUST NOT** imposes a binding prohibition, and **MAY** identifies a permitted action or authorized discretion.

Part I - Agreement Framework

1. Purpose

1.1 This Agreement governs the Contributor’s security obligations when participating in XPScerpto contribution activities.

1.2 Its purpose is to protect credentials, Restricted Information, Security-Sensitive Information, repositories, Workspaces, artifacts, systems, evidence, and vulnerability-handling processes from unauthorized access, disclosure, alteration, misuse, or destruction.

1.3 This Agreement establishes contributor-facing security boundaries. It does not replace a complete security policy, vulnerability-disclosure policy, incident-response plan, provider-security standard, or internal operational runbook.

1.4 This Agreement does not grant authorization to test a system, access a repository, process a dataset, retain a credential, disclose a Security Finding, or act outside an applicable AccessGrant and Source Scope.

1.5 A security control, access state, or technical capability does not create legal or operational authority merely because it is visible, technically possible, or available through a provider.

2. Scope

2.1 This Agreement binds the human Contributor who affirmatively accepts it.

2.2 It applies to contribution-related access, Workspaces, repositories, source code, artifacts, evidence, credentials, security testing, vulnerability reporting, remediation, provider interactions, and incident handling.

2.3 It applies to security-sensitive work conducted through an XPScerpto-controlled environment and to materially connected activity conducted through an external provider, local tool, communication channel, or organization environment when that activity uses XPScerpto access, information, credentials, or authorization.

2.4 This Agreement applies whether the Contributor is acting individually or in connection with an employer, university, research institution, customer, sponsor, or other organization.

2.5 An organizational, employment, academic, or research relationship does not enlarge the Contributor’s authority, create access, authorize testing, or permit disclosure of XPScerpto information.

2.6 The Code of Conduct governs interpersonal misconduct, retaliation, coercion, and abuse of authority. This Agreement governs the security boundary and security-specific obligations; the same conduct may be relevant under both documents.

3. Governing Security Principles

3.1 Security authorization is explicit, limited, current, and revocable. It is not inferred from technical capability, prior access, role title, organizational affiliation, or the absence of a technical block.

3.2 The narrower valid boundary controls. If a provider, tool, or local state appears to permit more than the AccessGrant or Source Scope allows, the Contributor remains limited to the authorized boundary.

3.3 Access and disclosure are separate permissions. Authorization to access information within XPScerpto does not, by itself, authorize transmission, publication, copying, or disclosure of that information to another person, organization, service, or system.

3.4 A claimed vulnerability, generated proof of concept, or proposed remediation is not a confirmed security result until validated through the process required for the affected activity.

3.5 Security evidence MUST describe events that actually occurred. A simulation, reconstruction, generated log, or illustrative screenshot does not become Execution Evidence through labeling, confidence, or repetition.

3.6 Protective security action may be required before a final determination of fault. A temporary freeze, deny, isolation, or revocation used to contain risk is not, by itself, a disciplinary finding.

4. Definitions

4.1 AccessGrant

An **AccessGrant** is the XPScerpto-controlled record that identifies the resources and actions available to a Contributor, together with the applicable limits, conditions, start and expiry states, and any external-provider confirmation required for access.

4.2 Agreement

The **Agreement** means the exact XPScerpto Contributor Security Agreement version identified by its Agreement ID, version, and canonical document SHA-256 when presented for acceptance.

4.3 Authorized Security Testing

Authorized Security Testing is security testing expressly permitted for the identified system, environment, methods, time period, and Source Scope under a current AccessGrant or other binding authorization. General contributor access, public availability, or possession of a tool is not Authorized Security Testing.

4.4 Contractual Requirement

A **Contractual Requirement** is this Agreement or another agreement, policy, code, task-specific term, security instruction, or organization- or project-specific obligation that is binding on the Contributor and applies to the activity in question.

4.5 Contributor

A **Contributor** is the human individual who accepts this Agreement and uses, receives, controls, or is identified as responsible for access, information, security work, or a contribution governed by it.

4.6 Credential

A **Credential** is information or material capable of authenticating, authorizing, signing, decrypting, or establishing access, including a password, token, API key, private key, session secret, recovery code, certificate private material, or comparable secret.

4.7 Execution Evidence

Execution Evidence is a record of an event that actually occurred, produced or confirmed through an authorized process and associated with the relevant source, artifact, system, environment, or Submission version. Generated or reconstructed material is not Execution Evidence when the represented event did not occur.

4.8 Operational Determination

An **Operational Determination** is a current decision or recorded state made under existing Contractual Requirements, such as an AccessGrant state, Source Scope, Workspace state, provider confirmation, security classification, freeze, revocation, testing authorization, Verification result, or reporting eligibility. It applies existing requirements without amending this Agreement.

4.9 Restricted Information

Restricted Information is information whose access, use, processing, retention, or disclosure is limited by a

Contractual Requirement or Operational Determination. It can include access-restricted source code, private repository information, personal data, contributor-private data, customer or organization information, restricted datasets, internal documents or logs, Credentials, non-public vulnerabilities, private security reports, and non-public review content.

4.10 Security Finding

A **Security Finding** is a suspected or confirmed weakness, vulnerability, exposure, misconfiguration, control failure, or security-relevant behavior affecting a system, artifact, process, or dependency. A Security Finding is not confirmed merely because it was generated, predicted, or described by a tool or person.

4.11 Security Incident

A **Security Incident** is an event or suspected event involving unauthorized access, disclosure, alteration, loss, misuse, compromise, or material security-control failure affecting XPScerpto contribution activity, information, Credentials, systems, artifacts, evidence, or provider access.

4.12 Security-Sensitive Information

Security-Sensitive Information is Restricted Information requiring heightened handling because it concerns Credentials, security controls, non-public vulnerabilities, exploitability, incident response, private security reports, security-restricted source code, or another comparable security matter.

4.13 Source Scope

A **Source Scope** is the current authoritative boundary for a task or security activity, identifying the

repositories, branches, paths, files, artifacts, systems, environments, datasets, methods, permitted actions, and exclusions.

4.14 Submission

A **Submission** is the versioned record or package through which a contribution, Security Finding, remediation, evidence item, or related artifact is presented for scope checks, Verification, review, or decision.

4.15 Verification

Verification is an authorized process that evaluates a Security Finding, remediation, Submission, artifact, or result against identified checks or requirements. Verification is distinct from authorization, access, acceptance, and final disposition.

4.16 Version-Bound Acceptance Receipt

A **Version-Bound Acceptance Receipt** is an auditable record associating an affirmative acceptance with the Contributor’s identity, the Agreement ID, the exact Agreement version, the canonical document SHA-256, the acceptance time, the acceptance context, and the applicable agreement policy version.

4.17 Workspace

A **Workspace** is a task-bound technical environment or resource made available under an AccessGrant and any provider confirmation required for access.

Part II - Contributor Security Obligations

5. Baseline Security Duties

5.1 The Contributor MUST use XPScerpto systems, access, information, and tools only for an authorized contribution purpose and within the applicable Contractual Requirements.

5.2 The Contributor MUST maintain the confidentiality of Credentials and Restricted Information and MUST prevent unauthorized persons or systems from using the Contributor’s access.

5.3 The Contributor MUST NOT disable, evade, degrade, conceal, or misrepresent a security control, logging requirement, access boundary, source-scope control, malware check, secret check, or Verification gate.

5.4 The Contributor MUST NOT exploit a technical gap, stale provider state, excessive permission, missing client-side restriction, or operational delay to perform an action that is not authorized.

5.5 The Contributor MUST accurately describe material security actions, results, limitations, and failures and MUST NOT represent an unexecuted or inconclusive activity as successful or verified.

5.6 If a requirement is unclear, unavailable, or in conflict, the Contributor MUST stop the affected security-sensitive action and seek an authorized determination rather than assume the broader permission.

6. AccessGrant, Source Scope, and Least Authority

6.1 The Contributor MUST remain within the exact resources, actions, methods, environment, and period authorized by the AccessGrant and Source Scope.

6.2 The Contributor MUST NOT access, enumerate, probe, copy, modify, test, or retain a repository, system, dataset, account, environment, artifact, or secret outside

that boundary.

6.3 An AccessGrant for one task, organization, customer, system, or environment MUST NOT be used for another.

6.4 The Contributor MUST NOT attempt to expand a Source Scope, extend an expiry, reactivate access, change an approval, or bypass a freeze or revocation through a client request, provider interface, alternate account, automation, or another person.

6.5 If an external provider exposes broader access than the AccessGrant permits, the Contributor MUST treat the broader access as unauthorized, stop using it, and report the discrepancy.

6.6 The Contributor MUST NOT rely on a cached session, local clone, saved link, copied artifact, retained Credential, or delayed provider revocation after the internal authorization has expired, been suspended, frozen, or revoked.

6.7 The Contributor MUST NOT grant or share XPScerpto access with an employer, colleague, academic supervisor, student, contractor, collaborator, AI agent, or another person unless an applicable authorization expressly permits that use.

7. Credentials and Authentication Material

7.1 The Contributor MUST protect each Credential against disclosure, reuse, copying, unauthorized storage, and unauthorized access.

7.2 The Contributor MUST NOT place a live Credential in source code, a Submission, issue, review thread, chat, screenshot, test fixture, documentation, AI prompt, model context, build log, terminal transcript, or another artifact not authorized to contain it.

7.3 The Contributor MUST NOT transmit a live Credential to an external AI service, public scanning service, unapproved debugging service, or another external processor.

7.4 A Credential may be processed within a controlled environment only when a separate authorization expressly permits the relevant Credential type, system, purpose, and handling method.

7.5 The Contributor MUST NOT share a personal session or Credential, use another person’s Credential, or allow another person to operate under the Contributor’s identity.

7.6 The Contributor MUST report suspected Credential exposure, loss, misuse, unauthorized copying, or compromise through the designated security channel and MUST cease further use when instructed or when continued use would increase the risk.

7.7 Revocation or rotation of a Credential does not authorize disclosure of the former value or retention beyond an applicable requirement.

8. Restricted Repositories, Artifacts, and Information

8.1 The Contributor MUST use Restricted Information only for the authorized contribution activity and only within the environments and channels permitted for its classification.

8.2 Authorization to access Restricted Information within XPScerpto does not authorize disclosure to an external service, personal repository, public issue tracker, portfolio, publication, conference, employer, university, sponsor, or another person.

8.3 The Contributor MUST minimize Restricted Information in Submissions, examples, screenshots, logs, reports, discussions, and evidence.

8.4 The Contributor MUST NOT copy or synchronize a restricted repository or artifact to an unauthorized device, account, storage service, backup, mirror, fork, or organization system.

8.5 The Contributor MUST NOT use Restricted Information to train, fine-tune, evaluate, or provide context to an AI system unless the applicable AI-processing policy expressly authorizes the information classification, environment, provider, and use case.

8.6 A transformed, summarized, redacted, encoded, or generated representation remains restricted if it reveals or permits reconstruction of Restricted Information.

8.7 If an authorized channel cannot receive information of the required classification, the Contributor MUST stop the transmission and obtain a secure routing determination. The absence of a working channel does not authorize public or lower-classification disclosure.

9. Workspaces, Local Environments, and Tools

9.1 The Contributor MUST use a Workspace and associated tools only while the relevant access and Workspace state permit the activity.

9.2 The Contributor MUST NOT launch, continue, or resume work in a Workspace that is frozen, expired, revoking, revoked, archived, or otherwise denied for use.

9.3 The Contributor MUST NOT introduce unauthorized remote-access software, persistence, hidden services, covert channels, credential collection, or monitoring into a Workspace or contribution environment.

9.4 The Contributor MUST NOT disable endpoint, network, logging, malware, secret-detection, policy, or audit controls required for the environment.

9.5 A local tool that transmits telemetry, diagnostics, crash reports, logs, prompts, source, or artifacts outside the controlled environment is subject to the same external-processing restrictions as the receiving service.

9.6 The Contributor MUST verify a security tool, dependency, image, package, or scanner before use when its identity or behavior materially affects the security of the activity.

9.7 The Contributor MUST NOT use an unverified or hallucinated package, command, exploit module, rule set, or security reference solely because a tool or model recommended it.

10. Security Testing Authorization

10.1 The Contributor MUST conduct security testing only as Authorized Security Testing.

10.2 Authorization for ordinary development, review, source access, or Workspace use does not by itself authorize vulnerability scanning, exploitation, credential testing, denial-of-service activity, persistence, lateral movement, data extraction, or testing of another account or environment.

10.3 The Contributor MUST comply with the systems, methods, targets, intensity, data handling, time limits, and stop conditions established for the authorized test.

10.4 The Contributor MUST NOT test a production system, third-party system, customer environment, external provider, or unrelated asset unless that exact activity is

authorized.

10.5 The Contributor MUST NOT continue testing after expiry, revocation, a stop instruction, discovery of an out-of-scope system, or an event that creates an uncontained risk.

10.6 The Contributor MUST NOT use a test to obtain unrelated data, maintain unauthorized access, prove status, retaliate, pressure a decision-maker, or secure an unrelated benefit.

10.7 This Agreement does not create safe harbor, a bug bounty, immunity, permission to violate third-party terms, or authorization beyond the express scope of the applicable security process.

11. Security Findings and Responsible Reporting

11.1 The Contributor MUST report a Security Finding through the channel designated for the affected activity and classification.

11.2 The report MUST accurately distinguish suspected behavior, reproduced behavior, confirmed impact, untested hypotheses, and information that remains unknown.

11.3 A Security Finding generated or suggested by an AI system, scanner, static analyzer, model, or another tool is unconfirmed until independently validated as required by the applicable process.

11.4 The Contributor MUST NOT represent a generated proof of concept as verified exploitation unless the relevant action was actually performed within authorization and supported by the required Execution Evidence.

11.5 The Contributor MUST include only the Restricted Information necessary for triage and MUST submit sensitive

evidence through the channel authorized for its classification.

11.6 The Contributor MUST NOT publish, forward, demonstrate, or disclose a non-public Security Finding outside the authorized process.

11.7 The Contributor MUST NOT contact an affected customer, user, organization, provider, researcher, press outlet, regulator, or public forum on XPScerpto’s behalf unless expressly authorized.

11.8 The Contributor MAY state uncertainty and is not required to establish final severity or liability before making a good-faith report.

12. Private Handling and Disclosure Boundaries

12.1 Non-public Security Findings, exploit details, affected source, Credentials, reproduction data, and remediation status are Security-Sensitive Information.

12.2 The Contributor MUST comply with the applicable private-reporting, triage, coordination, and disclosure requirements and MUST NOT infer a publication right from the passage of time, silence, disagreement, or the absence of a technical block.

12.3 This Agreement does not establish an embargo period, public-disclosure deadline, coordinated-disclosure timetable, or mandatory public credit. Those matters require a separate security-disclosure policy or written authorization.

12.4 The Contributor MUST NOT use possession of a Security Finding to threaten disclosure, demand payment or another unrelated benefit, force a statement, obtain access, manipulate review, or coerce a decision.

12.5 A good-faith disagreement about severity, reproducibility, scope, or remediation is not by itself retaliation or suppression. The parties remain subject to the Code of Conduct and applicable security process.

12.6 If a reporting channel is unavailable, the Contributor MUST preserve confidentiality and use another channel authorized for Security-Sensitive Information or request secure-routing instructions.

12.7 Nothing in this Agreement restricts a disclosure that mandatory law protects or requires. A Contributor relying on such a rule MUST act on a good-faith basis, limit the disclosure to what the rule permits, and MUST NOT claim to speak for XPScerpto without authorization.

13. Security Evidence and Reproducibility

13.1 Security evidence MUST be bound to the relevant system, version, source, environment, time, and authorized activity to the extent required by the applicable process.

13.2 The Contributor MUST NOT fabricate, alter, omit, misattribute, or reuse terminal output, logs, screenshots, network traces, proof-of-concept results, provider receipts, vulnerability evidence, or Verification results in a manner that misrepresents what occurred.

13.3 A simulated, illustrative, or reconstructed artifact MAY be provided only when the context permits it, it is clearly identified as non-executed, and it is not used to satisfy an Execution Evidence requirement.

13.4 The Contributor MUST preserve material limitations, failures, partial reproduction, environmental differences, and uncertainty in a security report or evidence summary.

13.5 The Contributor MUST NOT expose unrelated source, secrets, personal data, customer information, internal

infrastructure, or another Contributor’s information in security evidence.

13.6 A stale, superseded, or differently scoped result MUST NOT be represented as current for a later system, version, Submission, or remediation.

13.7 A client-side result, model output, or locally created status does not become authoritative merely because it resembles a provider or Verification record.

14. Remediation and Verification

14.1 A proposed remediation is not a verified fix until it is evaluated against the affected version, the relevant failure or threat condition, required regression checks, and any security Verification required for the activity.

14.2 The Contributor MUST NOT represent an AI-generated, tool-generated, or manually proposed change as verified remediation solely because it appears plausible or passes an unrelated test.

14.3 The Contributor MUST disclose known residual risk, incomplete coverage, untested assumptions, and compatibility effects material to remediation review.

14.4 Verification of a remediation MUST remain associated with the exact source, artifact, build, environment, and Submission version evaluated.

14.5 A passing security check does not by itself establish admission, release approval, final risk acceptance, or permission to disclose the finding.

14.6 If the required verification environment or process is unavailable, the Contributor MUST report that state and MUST NOT substitute unsupported local output for the required result.

15. Malicious, Destructive, and Deceptive Activity

15.1 The Contributor MUST NOT introduce malware, a backdoor, credential theft, unauthorized telemetry, covert persistence, destructive logic, hidden access, data exfiltration, or another malicious capability into a contribution, Workspace, tool, dependency, or test environment.

15.2 The Contributor MUST NOT intentionally damage availability, corrupt data, interfere with another person’s work, consume resources abusively, or trigger destructive behavior outside Authorized Security Testing.

15.3 The Contributor MUST NOT conceal malicious or security-relevant behavior through obfuscation, misleading naming, generated code, nested artifacts, disabled tests, altered logs, or another deceptive technique.

15.4 The Contributor MUST NOT create or submit a false vulnerability, fabricated exploit, deceptive proof of concept, manipulated severity claim, or invented security evidence.

15.5 Possession or creation of dual-use security code is not, by itself, a violation when the code is authorized, scoped, handled, and represented accurately. Its use remains limited by this Agreement and the applicable security process.

16. Access Expiry, Revocation, and Retained Copies

16.1 The Contributor MUST stop using an AccessGrant, Credential, Workspace, repository, or provider access when it expires, is suspended, frozen, revoked, or otherwise denied.

16.2 The Contributor MUST comply with authorized

instructions concerning return, deletion, destruction, transfer, or preservation of local copies, artifacts, Credentials, and Restricted Information after access ends.

16.3 The Contributor MUST NOT retain a copy for portfolio, research, training, benchmarking, publication, future work, dispute leverage, or personal reference unless a Contractual Requirement expressly permits that retention.

16.4 The Contributor MUST NOT erase, alter, or destroy a record that an applicable legal, security, audit, investigation, or evidence-preservation requirement directs the Contributor to preserve.

16.5 This Agreement does not establish a universal retention or deletion period. The applicable security, privacy, project, legal, and evidence-preservation requirements govern the disposition of each category of information.

16.6 Completion of a task or Submission does not authorize continued use of access or Restricted Information beyond the activity for which it was provided.

17. Security Incidents and Containment

17.1 The Contributor MUST report a Security Incident without avoidable delay after discovery through the designated security channel.

17.2 A report MUST identify, to the extent known and safe to provide, the affected access, system, artifact, information category, time, observed behavior, containment already performed, and facts that remain uncertain.

17.3 The report MUST exclude unrelated Restricted Information and MUST use a channel authorized for the information’s classification.

17.4 Within the Contributor’s existing authority, the Contributor MUST stop the affected action, stop unauthorized disclosure or propagation, isolate an affected process or tool when authorized, preserve relevant factual records, and avoid altering evidence in a way that obscures the incident.

17.5 The Contributor MUST NOT conduct additional intrusive testing, access another system, contact affected persons, or disclose the incident publicly unless authorized as part of containment or investigation.

17.6 When an applicable Contractual Requirement validly requires the Contributor’s participation in incident review or remediation, the Contributor MUST provide truthful, relevant information and the cooperation specified by that requirement.

17.7 Incident reporting does not by itself determine fault, liability, misconduct, or sanction.

18. Security Research, Coercion, and Good-Faith Activity

18.1 A Contributor does not violate this Agreement merely by reporting a serious Security Finding, demonstrating material impact within Authorized Security Testing, disagreeing with a security assessment, or requesting remediation through an authorized channel.

18.2 The Contributor MUST NOT use a Security Finding, Credential, access condition, or disclosure threat to extort, coerce, intimidate, retaliate, obtain an unrelated benefit, or manipulate a contribution or review decision.

18.3 The Contributor MUST NOT knowingly submit a false security report, fabricate supporting evidence, or use security reporting as a tool of harassment, retaliation, or deliberate disruption.

18.4 A report is not false merely because it is disputed, partially mistaken, or not substantiated after review. Good faith is assessed from the information honestly believed and reasonably available to the reporting person at the time.

18.5 Retaliation for good-faith security reporting or authorized participation is prohibited under the Code of Conduct. That protection does not excuse independently established misconduct or unauthorized testing.

Part III - Governance and Consequences

19. Protective Security Measures

19.1 When existing authority permits it, a protective security measure MAY be used to contain an immediate or developing risk involving access, Credentials, Restricted Information, evidence integrity, a Workspace, a provider, or an affected system.

19.2 A protective measure can include temporary deny, freeze, isolation, Credential rotation, session invalidation, access restriction, artifact quarantine, or suspension of an affected workflow.

19.3 A protective measure is not, by itself, a final determination that the Contributor violated this Agreement.

19.4 A provider-revocation delay or convergence failure does not restore internally denied authority. The Contributor MUST continue to treat the affected access as unavailable.

19.5 The existence, duration, and scope of a protective measure remain governed by the authority and process under which it is imposed. This Agreement does not create a new

emergency power.

20. Non-Compliance, Remediation, and Enforcement

20.1 A violation MAY result in measures available under an applicable Contractual Requirement. Depending on the established facts and existing authority, those measures can include:

- a direction to stop an affected activity;
- correction, replacement, quarantine, or removal of affected material or evidence;
- invalidation or repetition of security testing, Verification, review, or a Submission;
- Credential rotation, session invalidation, Workspace freeze, or restriction of relevant access;
- suspension or revocation of an affected contribution flow or AccessGrant; or
- referral to an authorized security, privacy, conduct, intellectual-property, organization, legal, or incident process.

20.2 This Agreement does not create an investigation, suspension, revocation, disciplinary, employment, academic, or legal authority that is not otherwise available under an applicable agreement, policy, role, or law.

20.3 A scanner result, model output, automated alert, client-side status, or unsupported allegation is not sufficient by itself to establish a final violation or sanction.

20.4 Remediation does not retroactively authorize an out-of-scope action, make fabricated evidence genuine, or remove an independently established violation.

20.5 A final measure under this Agreement MUST remain connected to the established conduct, current security

risk, affected access or activity, and authority actually available.

21. Relationship with Other Requirements

21.1 This Agreement operates with the Code of Conduct, Contribution Policy, intellectual-property agreement, AI-Assisted Contributions Agreement, privacy acknowledgment or notice, and applicable task-, project-, organization-, provider-, and environment-specific requirements.

21.2 Each Contractual Requirement governs its assigned subject matter and scope. An express precedence provision in an applicable agreement or policy controls to the extent stated.

21.3 The Contributor MUST comply with every applicable requirement that can be performed consistently within its own scope.

21.4 If two applicable requirements cannot both be satisfied, the Contributor MUST stop the affected action and request a determination through the legal, policy, security, privacy, review, or operational process designated for the conflict.

21.5 Pending resolution, the Contributor MUST NOT choose an interpretation that expands access or Source Scope, permits additional testing, weakens a security or privacy control, removes required Verification or reviewer independence, or authorizes disclosure.

21.6 An Operational Determination implements or records the application of an existing Contractual Requirement. It does not amend this Agreement or create a concealed contractual obligation.

22. Governing Language and Pending Legal Framework

22.1 The governing legal text of this Agreement is the English canonical version. A translation is informational and cannot amend or outrank it.

22.2 The governing law, competent court or other forum, and dispute-resolution process have not received final legal designation from XPScerpto.

22.3 The language, security subject matter, publication location, system location, or technical delivery of this Agreement does not select any governing law, jurisdiction, forum, or dispute process by implication.

22.4 This Agreement is not eligible for activation as a published contractual version until XPScerpto either designates those matters expressly or establishes that binding XPScerpto general terms or a master agreement applicable to the Contributor expressly supplies them.

22.5 Nothing in this Section limits a mandatory rule of law that applies regardless of contractual designation.

Part IV - Agreement Lifecycle

23. Version-Bound Acceptance

23.1 Acceptance applies only to the Agreement ID, exact Agreement version, governing language, and canonical document SHA-256 presented through the authoritative acceptance process.

23.2 Acceptance requires an affirmative action by the Contributor. Silence, continued account use, an unrelated action, a preselected control, or action by another person or automated system is not acceptance.

23.3 A Version-Bound Acceptance Receipt evidences a successful acceptance only for the recorded version; it cannot be used as acceptance of any earlier, later,

translated, or modified text.

23.4 Authoritative metadata records the SHA-256 of the frozen canonical source calculated under the approved canonicalization profile. A value supplied by a client or inconsistent with that source cannot identify the Agreement.

23.5 A failed, incomplete, conflicting, or client-only acceptance attempt is not acceptance.

24. Agreement Status, Material Change, and Historical Integrity

24.1 The authoritative agreement metadata identifies the current lifecycle status of each Agreement version.

24.2 A withdrawn version is not eligible for new acceptance.

24.3 A superseded version is historical rather than current. The governing agreement-lifecycle requirement decides whether it can receive any further acceptance.

24.4 Acceptance of an earlier version is not acceptance of a later version.

24.5 A change classified as material under the agreement-lifecycle requirements MAY require affirmative acceptance of a new version before the Contributor may perform security-sensitive activities for which that version is a prerequisite.

24.6 Historical acceptance and decline records remain associated with the exact version and canonical hash recorded and are not rewritten by supersession, withdrawal, later acceptance, account closure, or access loss.

25. Declining the Agreement

25.1 The Contributor MAY decline this Agreement or a replacement version presented for acceptance.

25.2 A decline is not acceptance and MUST NOT be recorded, displayed, or inferred as acceptance.

25.3 Declining MAY prevent access to a task, Workspace, repository, security activity, Submission type, or contribution workflow for which acceptance of the active Agreement is an established prerequisite.

25.4 Declining does not automatically close the Contributor’s account, terminate contributor status, erase identity data, or remove unrelated functions unless another Contractual Requirement expressly provides that result.

25.5 The acceptance process MUST display the known consequence for the affected workflow before the Contributor confirms a decline.

25.6 If the Contributor later accepts, the system records a new Version-Bound Acceptance Receipt for the version then eligible; the earlier decline remains historical.

26. Acceptance Statement

Through affirmative acceptance of this exact Agreement version using the XPScerpto acceptance control, the Contributor confirms that:

1. the Agreement ID, Agreement version, governing language, and canonical document SHA-256 presented for acceptance identify the Agreement;
2. the Contributor has reviewed this Agreement;
3. the Contributor agrees to comply with it for security-sensitive contribution activities governed by it;

4. access, technical capability, a provider state, or possession of a Security Finding does not create authority beyond the applicable AccessGrant, Source Scope, and Authorized Security Testing;
5. the Contributor will protect Credentials, Restricted Information, Security-Sensitive Information, and security evidence as required; and
6. the acceptance may be recorded as a Version-Bound Acceptance Receipt.

Reporting Through the Existing XPScerpto System

Security findings and security incidents MUST be submitted through the existing XPScerpto platform reporting system using the security-report category. A conduct report MUST NOT be relabeled as a security report to bypass the conduct process. The reporting system’s access, isolation, restricted-information, receipt, follow-up, and audit controls remain authoritative.

Version and Historical Integrity

Acceptance applies only to this exact Agreement version and its canonical SHA-256 recorded by the authoritative XPScerpto service. A material change requires a new version and, when the applicable policy requires it, a new acceptance. A historical version, acceptance, decline, or receipt MUST NOT be rewritten as applying to different text, a different hash, or a different legal operator. New acceptance of a `SUPERSEDED` or `WITHDRAWN` version is prohibited. Agreement acceptance does not grant access, verified capability, trust, or a Workspace.