

## Allgemeine Prüfbestimmungen NTC

Version 2.0, 9. April 2024

## Inhaltsverzeichnis

1. Anwendungsbereich	3
2. Auftragserteilung und Prüfbericht	3
3. Prüfprozess	3
4. Verwendung des Prüfberichts	4
5. Kommunikation und "responsible disclosure"	4
6. Gebühren	4
7. Gewährleistung und Haftung	4
8. Vertraulichkeit und Datenschutz	5
9. Geistige Eigentumsrechte	5
10. Aktualisierung	5
11. Dauer und Auflösung	5
12. Schlussbestimmungen	5

## 1. Anwendungsbereich

- 1.1. Das Nationale Testinstitut für Cybersicherheit NTC ("NTC") prüft Hard- und Software sowie vernetzte Komponenten auf ihre Cybersicherheit. Das NTC fusst auf einer öffentlich-privaten Trägerschaft, bestehend aus Partnern der öffentlichen Hand und Unternehmungen aus der Privatwirtschaft.
- 1.2. Die vorliegenden Allgemeinen Prüfbestimmungen gelten für die zwischen dem NTC und ihren Auftraggebern abgeschlossenen Verträgen betreffend die Prüfung von Hard- und/oder Softwarekomponenten. Ergänzende oder abweichend vereinbarte Bestimmungen bleiben vorbehalten, sofern sie explizit als solche bezeichnet und gegenseitig in Textform festgehalten sind.

## 2. Auftragserteilung und Prüfbericht

- 2.1. Prüfaufträge werden vom Auftraggeber auf der Basis der vom NTC zur Verfügung gestellten Formatvorlagen erteilt, welche den Prüfumfang und die relevanten Sicherheitskriterien enthalten. Das NTC behält sich eine Ablehnung von Prüfungsaufträgen jederzeit vor.
- 2.2. Das NTC erstellt einen Prüfbericht zuhanden des Auftraggebers, dessen Verwendung nachstehend in Ziffer 4 geregelt ist. Der Prüfbericht wird elektronisch erstellt und dem Auftraggeber als PDF, sowie auf dessen Wunsch hin auch schriftlich zugestellt.

## 3. Prüfprozess

- 3.1. Das NTC nimmt Prüfaufträge aus der Privatwirtschaft, der Verwaltung und anderen Organisationen (z.B. Hochschulen, NGO) entgegen.
- 3.2. Das NTC stellt durch seine technische Fachgruppe sicher, dass die organisatorischen und technischen Rahmenbedingungen zur Durchführung von Prüfungen vorliegen. Dies beinhaltet z.B. die Abklärung zum Vorhandensein der genügenden vertraglichen Aspekte zwischen den betroffenen Stakeholdern, die Plausibilität der Tiefe von Prüfspezifikationen sowie die Auswahl von Standards und von geeigneten Experten. Das NTC arbeitet als Prüfinstitut mit eigenen Experten und zieht nach Bedarf externe Prüfer bei.
- 3.3. Die Prüfvorgänge folgen einem vom NTC definierten Prozess und werden dokumentiert. Die zu jedem Prüfauftrag erforderliche Prüfspezifikation regelt individuell, welche Fragestellungen mindestens Bestandteil der Prüfung sind. Prüfspezifikationen können von den Vertragspartnern im Verlauf der Prüfung im gegenseitigen Einverständnis erweitert werden. Die Prüfspezifikationen können auf existierende Standards verweisen.
- 3.4. Der Auftraggeber ist verpflichtet, dem NTC bzw. ihren Prüfern die für die Durchführung der Prüfung erforderlichen Materialien, Unterlagen und Auskünfte frei von Rechten Dritter vollständig und wahrheitsgemäss zugänglich zu machen. Weitere Mitwirkungspflichten werden im Prüfauftrag vereinbart.
- 3.5. Für jede durchgeführte Prüfung wird ein detaillierter Prüfbericht erstellt. Dieser enthält die tatsächlich durchgeführten Schritte einschliesslich deren Nachweise sowie die festgestellten Ergebnisse. Jede Schwachstelle wird in eine der Kategorien Critical, High, Medium, Low und Info eingeteilt und es wird jeweils eine Handlungsempfehlung vorgeschlagen. Der Prüfbericht wird digital über einen sicheren Kanal übermittelt und wird mindestens 5 Jahre manipulationssicher und vertraulich im NTC aufbewahrt werden. In den Prüfspezifikationen können andere Fristen vereinbart werden.

## 4. Verwendung des Prüfberichts

- 4.1. Die dem Auftraggeber unter dem Namen und dem Logo von NTC ausgehändigten Prüfberichte gelten als zentrale Lieferobjekte und können vom Auftraggeber in unveränderter Form frei verwendet werden. Eine anderweitige Nutzung des Namens oder Logos des NTC ist nicht gestattet. Stellt NTC eine missbräuchliche oder den Inhalt verfälschende Nutzung des Prüfberichtes durch den Auftraggeber fest, kann sie diesem das Recht zum weiteren Gebrauch des Prüfberichtes entziehen. Die Prüfergebnisse gehören dem NTC und werden von diesem grundsätzlich im Rahmen der vorliegenden Allgemeinen Prüfbestimmungen verwendet.
- 4.2. Das NTC kann die Ergebnisse aus den Prüfungen, in anonymisierter Form, weiteren Organisationen zur Verfügung stellen, soweit mit dem Auftraggeber nichts Abweichendes vereinbart worden ist. Der Auftraggeber kann hierfür mit dem NTC eine finanzielle Abgeltung vereinbaren.

## 5. Kommunikation und "responsible disclosure"

- 5.1. Unter Einhaltung von rechtlichen Rahmenbedingungen werden Schwachstellen und die resultierenden Risiken wie folgt kommuniziert:
  - Alle identifizierten Schwachstellen werden dem Auftraggeber spätestens nach Beendigung des Prüfauftrags in Form des Prüfberichts mitgeteilt. Ist der Auftraggeber nicht der Hersteller, so wird der Auftraggeber zwar über die Existenz schwerwiegender Schwachstellen informiert, ohne jedoch technische Details zur Ausnutzbarkeit der Schwachstellen bekanntzugeben. In jedem Fall wird Hilfestellung zum Schutz vor Ausnutzen der Schwachstelle gegeben.
  - Schwachstellen, welche im Ermessen des NTC als schwerwiegend gelten (in der Regel Schwachstellen der Kategorie Critical und High), können inklusive einem anonymisierten Proof-of-Concept Exploit an den Hersteller des Prüfobjektes kommuniziert werden. Dabei gelten die jeweils aktuellen Rahmenbedingungen der NTC Vulnerability Disclosure Policy, welche unter [https://www.ntc.swiss/hubfs/NTC\\_Vulnerability\\_Disclosure\\_Policy.pdf](https://www.ntc.swiss/hubfs/NTC_Vulnerability_Disclosure_Policy.pdf) abgerufen werden kann und integrierenden Bestandteil der vorliegenden Prüfbestimmungen bildet.

## 6. Gebühren

- 6.1. Die Gebühr für die Prüfung wird in der jeweiligen Auftragserteilung vereinbart.
- 6.2. Rechnungen des NTC sind innert 30 Tagen nach Rechnungsdatum zahlbar. Alle Preise verstehen sich exklusive Mehrwertsteuer.

## 7. Gewährleistung und Haftung

- 7.1. Das NTC führt die Prüfungen durch qualifizierte Prüfer mit der gebotenen Sorgfalt und nach bestem Wissen und Gewissen durch. Es leistet keine Gewähr für die Korrektheit oder Werthaltigkeit von Prüfberichten und übernimmt keinerlei Ergebnisverantwortung.
- 7.2. Das NTC haftet im Rahmen der übernommenen Tätigkeit nur für Vorsatz und grobe Fahrlässigkeit. Soweit gesetzlich zulässig, wird jede weitere Haftung wegbedungen. Es haftet insbesondere nicht i) für Vollständigkeit oder Fehlerfreiheit von Prüfberichten; ii) dafür, dass der Prüfbericht von Dritten anerkannt wird; iii) für allfällige Schadenersatzansprüche Dritter, namentlich von Kunden der Auftraggeber; iv) für eine Nichterfüllung der Qualitätserwartungen Dritter; v) für Sicherheitsvorfälle jeglicher Art.
- 7.3. Der Auftraggeber hält NTC von jeglichen Ansprüchen Dritter frei, welche diese gegen das NTC im Zusammenhang mit der Erstellung oder der Verwendung des Prüfberichtes erheben.

## 8. Vertraulichkeit und Datenschutz

- 8.1. Die Parteien verpflichten sich gegenseitig, alle vertraulichen Informationen, welche sie im Zusammenhang mit der Auftragserteilung von der jeweils anderen Partei erhalten, geheim zu halten. Als vertrauliche Informationen gelten alle Informationen, die entweder als vertraulich bezeichnet werden oder aufgrund ihrer Natur als schützenswert erscheinen. Nicht als vertrauliche Informationen gelten Informationen, welche i) nachweislich im Zeitpunkt ihrer Mitteilung der anderen Partei bereits bekannt war; ii) ohne Zutun der empfangenden Partei offenkundig werden, oder iii) die empfangende Partei von gutgläubigen Dritten erhält, welche diese weder direkt noch indirekt von der offenlegenden Partei erhalten haben.
- 8.2. Das NTC verpflichtet sich insbesondere, die Geheimhaltungspflicht bezüglich vertraulicher Informationen, welche der Auftraggeber anlässlich der Prüfung offengelegt hat, den eingesetzten Prüfern schriftlich zu überbinden. Für den Zugriff auf besonders schützenswerte Informationen (wie z.B. Quellcode) können die Parteien weitergehende Geheimhaltungsbestimmungen vereinbaren.
- 8.3. Die Parteien verpflichten sich zur Einhaltung der anwendbaren Datenschutzgesetze.

## 9. Geistige Eigentumsrechte

Durch die vorliegende Vereinbarung werden vorbestehende geistige Eigentumsrechte der Parteien nicht berührt.

## 10. Aktualisierung

Prüfberichte gelten generell nur für eine bestimmte Versionsnummer (inkl. des Softwarestandes und der präsentierten Konfiguration) des Prüfobjektes. Eine Nachprüfung muss durch den Auftraggeber erneut initiiert werden. Der Prüfauftrag beinhaltet nicht automatisch die Prüfung aktualisierter Versionen des Prüfobjektes.

## 11. Dauer und Auflösung

Ein Prüfauftrag kommt mit dessen Annahme durch das NTC zustande und dauert bis zur Ablieferung des Prüfberichtes. Ein Prüfauftrag kann von jeder Partei nach den Bestimmungen des Auftragsrechts gekündigt werden. Eine Auflösung seitens NTC wegen gesetzlicher Vorgaben oder mangelnder Voraussetzungen seitens des Auftraggebers gilt nicht als Auflösung zur Unzeit.

## 12. Schlussbestimmungen

Die vorliegenden Allgemeinen Prüfbestimmungen finden auf jeden Prüfauftrag sowie die Nutzung des Prüfberichtes Anwendung, auch wenn der Auftraggeber in Bestellungen auf eigene AGBs verweist. Änderungen bedürfen der Schriftform. Die Vertragsbestimmungen unterstehen Schweizer Recht unter Ausschluss von Staatsverträgen. Ausschliesslicher Gerichtsstand ist Zug.