Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

# Leistungsvereinbarung 2026

## Bundesamt für Cybersicherheit (BACS)

**Bundesamt für Cybersicherheit**

Florian Schütz
Direktor

Bern, 28.11.2025

**Eidg. Departement für Verteidigung, Bevölkerungsschutz und Sport VBS**

Bundesrat Martin Pfister
Departementschef

Bern, 28.11.2025

Verteiler:
- Chef VBS
- Dir BACS
- GS VBS
- C Ressourcen VBS

**Beilagen:**

# A Projekte, Vorhaben und Ziele

| 0 | Zielstossrichtungen 2026-28 BA für Cybersicherheit (BACS) |
|---|---|

| Zielstossrichtung BACS 2026-2028 | Angestrebtes Resultat 2028 |
|---|---|
| 1. Das BACS nimmt Meldungen aus der Bevölkerung und der Wirtschaft zu Cyberbedrohungen, Schwachstellen und Cyberangriffen entgegen und wertet diese aus. | Das BACS ist bei Bevölkerung, Wirtschaft und Politik etabliert und anerkannt als erste Anlaufstelle bei Cyberbedrohungen. Meldungen erfolgen systematisch, schnell und effizient über definierte Kanäle. |
| 2. Das BACS unterstützt die kritischen Infrastrukturen subsidiär bei Cybervorfällen. | Das BACS unterstützt effektiv und zeitnah subsidiär bei Cybervorfällen. Betreiber kritischer Infrastrukturen (inkl. Behörden) greifen regelmässig auf diese Expertise zurück und bestätigen deren Mehrwert. |
| 3. Das BACS fördert den Informationsaustausch zu Cyberbedrohungen zwischen den relevanten Akteuren und trägt entscheidend dazu bei. | Das BACS bietet ein Informationssystem zum Informationsaustausch, welcher mit standardisierten Plattformen und etablierten Prozessen einen kontinuierlichen, vertrauensvollen und proaktiven Informationsfluss zwischen Betreibern kritischer Infrastrukturen (inkl. Behörden), Unternehmen und weiteren relevanten Akteuren ermöglicht. Bis Ende 2028 bringen die Betreiber kritischer Infrastrukturen ein Drittel der Informationen ein. |
| 4. Das BACS ist als zentrale Stelle für Sensibilisierung und Prävention in der Cybersicherheit etabliert. | Durch breit abgestützte Kampagnen und Sensibilisierungsmassnahmen wurde das Bewusstsein für Cyberrisiken in Bevölkerung und Wirtschaft merklich erhöht. |
| 5. Das BACS koordiniert die Umsetzung der Nationalen Cyberstrategie (NCS). | Die vom BACS verantworteten NCS-Massnahmen sind fristgerecht umgesetzt. Die Zusammenarbeit der beteiligten Akteure ist etabliert. Und die Fortschritte sowie die Wirksamkeit der NCS-Massnahmen sind transparent ausgewiesen. |

| 1 | Projekte und Vorhaben, welche im VA 2026 mit Integriertem Aufgaben- und Finanzplan (IAFP) 2027-29 publiziert werden |
|---|---|

| Nr | Projekte und Vorhaben | Zu erreichender Meilenstein 2026 |
|---|---|---|
| 1.1 | Ausbau der Informationsplattformen des BACS | Der Informationsaustausch zu Cyberbedrohungen ist mit standardisierten Plattformen und etablierten Prozessen des BACS verbessert.<br>Termin: 31.12.2026 |
| 1.2 | Bedarfsgerechte Anpassung der BACS-Dienstleistungen zur Unterstützung der kritischen Infrastrukturen | Die kritischen Infrastrukturen werden auch aufgrund der Erfahrungen aus der Meldepflicht mit einem verbesserten, gezielten Dienstleistungsportfolio zum Schutz vor Cyberbedrohungen unterstützt.<br>Termin: 31.12.2026 |
| 1.3 | Durchführung von nationalen Sensibilisierungsmassnahmen 2026 | Abschluss von zwei weiteren nationalen Sensibilisierungsmassnahmen in Zusammenarbeit mit nationalen oder internationalen Umsetzungspartnern.<br>Termin: 31.12.2026 |
| 1.4 | Umsetzung der Nationalen Cyberstrategie (NCS) | Planmässige Initialisierung oder Umsetzung der für 2026 geplanten NCS-Umsetzungsvorhaben mit Federführung des BACS. Der jeweilige Umsetzungsstand ist aus dem strategischen NCS-Controlling ersichtlich.<br>Termin: 31.12.2026 |

| 2 | BR Geschäfte 2026 (Publikation in BR Zielen 2026) |
|---|---|

| Nr | BR Geschäft | Zu erreichender Meilenstein 2026 |
|---|---|---|
| 2.1 | Subsidiarität und Cybersicherheit; Umsetzung der Handlungsmassnahme aus dem Bericht des Bundesrates in Erfüllung des Postulates 22.3368 Sicherheitspolitischen Kommission NR | Die Schaffung von rechtlichen Grundlagen wird geprüft, um Unterstützungsleistungen im Cyberbereich zu vereinfachen. Dem Bundesrat werden bis Ende 2026 Varianten zum weiteren Vorgehen unterbreitet. |
| 2.2 | Umsetzungsstand der Nationalen Cyberstrategie (NCS) | Der Bundesrat wird über den Umsetzungsstand der Nationalen Cyberstrategie informiert. |
| 2.3 | Vernehmlassung zur Gesetzgebung zur Cyberresilienz von Produkten mit digitalen Elementen zur Umsetzung der Motion 24.3810 Sicherheitspolitische Kommission SR | Eröffnung der Vernehmlassung. |

## 3 Weitere Ziele BACS 2026 (VBS-intern)

| Nr | Teilziel/Einzelmassnahmen | Zu erreichender Meilenstein 2026 |
|---|---|---|
| 3.1 | Über die wirksame Umsetzung der Nationalen Cyberstrategie (NCS) trägt das BACS zur Sicherheitspolitischen Strategie der Schweiz bei. | Die NCS-Berichterstattung zeigt den Bezug bzw. den Beitrag zur Umsetzung der sicherheitspolitischen Strategie auf. |
| 3.2 | Die BACS-Organisation ist auf eine effiziente Bearbeitung der Umsetzung der Meldepflicht für Cyberangriffe auf kritische Infrastrukturen ausgerichtet. | Alle Meldungen werden fristgerecht bearbeitet und angeforderte Unterstützungsleistungen der kritischen Infrastrukturen werden zeitnah erfüllt. |
| 3.3 | Der Informationsaustausch ist mittels Ausbaus der Informationsplattformen des BACS breit etabliert und effektiv. | Der Informationsaustausch mit Betreiberinnen kritischer Infrastrukturen ist qualitativ und quantitativ gestärkt. |
| 3.4 | Die Zusammenarbeit des BACS mit dem Kommando Cyber und dem SEPOS ist klar geregelt. | Die Prozesse für die Zusammenarbeit mit dem Kommando Cyber und dem SEPOS sind etabliert und eingespielt. |
| 3.5 | Das BACS informiert alle Zielgruppen aktiv und wirksam zu Cyberbedrohungen. | Das BACS veröffentlicht regelmässig für alle Zielgruppen Analysen und Empfehlungen zu Cyberbedrohungen. |

# 4. Zielvorgaben 2026 aus den Querschnittsbereichen VBS für alle VE VBS (Querschnittsziele)

## 4.1 Sicherheit, Steuerung und Portfoliomanagement

| Nr | Teilziel/Einzelmassnahmen | Messgrösse/Sollwert 2026 |
|---|---|---|
| 4.1.1 | Sicherheit | Sicherheitsmanagement: Bis Ende 2026 sind die folgenden Teilziele je Amt/Gruppe erreicht:<br>• Eingeführte Sicherheitsgovernance, ausgerichtet an den Weisungen der Sicherheit VBS (WESI) und der Sicherheitsgovernance VBS.<br>• Vollständige Erfassung der Assets im Asset-management nach den Weisungen Sicherheit VBS, Ziffer 20 bis Mitte 2026.<br>• Führung/Aktualisierung Verzeichnis über die Schutzobjekte in mindestens den folgenden Kategorien:<br>a. Informationen (Art. 7 Abs. 2 Bst. a ISV);<br>b. Informatikmittel (Art. 7 Abs. 2 Bst. b ISV);<br>c. Objekte (Gebäude, bauliche Einrichtungen und zugehörige Infrastruktur);<br>d. Personen mit sicherheitsrelevanten Funktionen.<br>Sicherstellung Konformität des Informationssicherheitsmanagementsystems (ISMS) nach dem Standard SN ISO/IEC 27001 und Meldung der Zielerreichung an den Sicherheitsverantwortlichen VBS (GS VBS). |
| 4.1.2 | Steuerung VBS<br>→ GS-VBS, Gruppe Verteidigung und armasuisse | Die Massnahmen zur Verbesserung der Projektsteuerung im VBS werden gemäss Projektauftrag des Chefs VBS im GS-VBS, in der Gruppe Verteidigung und bei der armasuisse bis Ende 2026 vollständig realisiert.<br>Dabei werden in Zusammenarbeit der drei Verwaltungseinheiten die notwendigen Grundlagen geschaffen, ein neues Steuerungsmodell eingeführt und ein wirksames Controlling etabliert. |
| 4.1.3 | Portfoliomanagement (PFM) | Die Governance PFM VBS wird umgesetzt.<br>Die VE-Portfolios sind vollständig aufgebaut und werden nach den Steuerungsvorgaben des GS-VBS geführt. |

## 4.2 Personal, Finanzen, Risikomanagement, BCM und Krisenmanagement

| Nr | Teilziel/Einzelmassnahmen | Messgrösse/Sollwert 2026 |
|---|---|---|
| 4.2.1 | Personal | Die Massnahmen zur Erhöhung des Frauenanteils am Personalbestand werden fortgeführt und überwacht. Die Entwicklung wird jährlich ausgewiesen. |
| 4.2.2 | Entlastungsprogramm EP 27 im VBS | Die für die Umsetzung der Massnahmen erforderlichen Voraussetzungen (z.B. Anpassungen gesetzlicher Grundlagen) werden geschaffen.<br>Die vorgegebenen Massnahmen werden umgesetzt. Der Umsetzungsstand wird regelmässig gegenüber Ressourcen VBS berichtet. |
| 4.2.3 | Risikomanagement, Business Continuity Management und Krisenmanagement | Risikomanagement:<br>• Das oberste Führungsgremium jeder Verwaltungseinheit (VE) führt mindestens zweimal jährlich einen strukturierten Risikodialog in Anwesenheit des Risiko-Coaches der VE durch.<br>• Einmal jährlich werden dem Chef VBS die identifizierten Risiken und deren Entwicklung im Rahmen einer ALS präsentiert.<br>Business Continuity Management (BCM):<br>• Die Business Impact Analyse (BIA), die BCM-Strategie und die Business Continuity Pläne werden jährlich gem. Vorgaben BCM Bund aktualisiert, vom obersten Führungsgremium der VE genehmigt und dem Chef VBS in einer ALS präsentiert.<br>• Mindestens ein BCM-Szenario wird jährlich erprobt.<br>Krisenmanagement:<br>Das Krisenmanagement wird überprüft und wenn nötig an die Verordnung über die Krisenorganisation der Bundesverwaltung (KOBV) angepasst. |
| 4.2.4 | Kultur und Werte VBS | Zwei Massnahmen im Bereich Kultur/Werte VBS* werden umgesetzt. Diese leisten einen konkreten Beitrag, damit die Mitarbeitenden das VBS als modernen und attraktiven Arbeitgeber wahrnehmen.<br>*(Offenheit, Respekt, Vertrauen, Mut, Weitsicht) |

### 4.3 Kommunikation

| Nr | Teilziel/Einzelmassnahmen | Messgrösse/Sollwert 2026 |
|---|---|---|
| 4.3.1 | Kommunikation | • Die Verwaltungseinheiten verfügen über eigene (vom Kommunikationskonzept VBS abgeleitete) Kommunikationskonzepte und kommunizieren diesen entsprechend.<br>• Die Verwaltungseinheiten fokussieren ihre Kommunikation auf das Kerngeschäft und kommunizieren die Stärken/Chancen des VBS. Sie informieren die Kommunikation VBS frühzeitig über ihre Planung.<br>• Die Verwaltungseinheiten setzen ihre Kommunikationsplanung selbständig um. Bei einer Kommunikation unter dem Lead der Kommunikation VBS unterstützen die Verwaltungseinheiten die Kommunikation VBS. |

# B Leistungsgruppen (LG)

## LG 1: Cybersicherheit

**ZIELE**

| | R 2024 | VA 2025 | VA 2026 | FP 2027 | FP 2028 | FP 2029 |
|---|---|---|---|---|---|---|
| **Cybersicherheit:** Das BACS leistet einen Mehrwert zum Schutz vor Cyberrisiken in der Schweiz. | | | | | | |
| – Einschätzung des Mehrwerts durch die Leistungsbezüger/-innen (Net Promoter Score) (Skala -100 bis +100) | 60 | 60 | 60 | 60 | 60 | 60 |

# C Reporting und Controlling

**Berichtstermine / Stichtage:**

- **31.03.: Teil A (Grundlage für Zwischenbeurteilung der Projekte, Vorhaben, Ziele)**
- **30.09.: Teil A (Grundlage für Schlussbeurteilung der Projekte, Vorhaben, Ziele)**
- **31.12.: Teil B (Grundlage für Jahresbeurteilung der Ziele und Messgrössen je LG)**

# D Anpassungen LVB

**Allfällige Anpassungen/Ergänzungen der LVB werden nachfolgend aufgeführt, datiert und begründet. Sie müssen von beiden unterzeichnenden Seiten eingesehen werden.**