

Allgemeine Informationssicherheitsbestimmungen für Lieferanten (AISB)

Version	1.0
Verbindlich für	Lieferanten der ewb
In Kraft ab	01.10.2026

1. Zweck und Geltungsbereich und vertragliche Einbindung

Diese Bestimmungen legen die allgemeinen Informationssicherheitsanforderungen fest, die Lieferanten bei der Teilnahme an Beschaffungsverfahren sowie bei der Erbringung von Leistungen für Energie Wasser Bern («ewb») einzuhalten haben.

Sie gelten ab ihrer ausdrücklichen Annahme durch den Lieferanten. Die Annahme kann insbesondere im Rahmen einer Offertanfrage, einer öffentlichen Ausschreibung, einer Bestellung oder eines schriftlichen Vertrags erfolgen. Die Annahme im Rahmen eines Beschaffungsverfahrens begründet keinen Anspruch auf Zuschlag oder Vertragsabschluss.

Werden Leistungen ohne separate Vertragsurkunde gestützt auf eine Offerte des Lieferanten und deren Annahme oder Bestätigung durch ewb bezogen, gelten diese Bestimmungen zusammen mit den in der Offertanfrage, Offerte, Annahmeerklärung oder Bestellung bezeichneten AEB IKT ewb und AGB SIK.

Wird mit dem Lieferanten eine Vertragsurkunde abgeschlossen, bilden diese Bestimmungen in der in der Vertragsurkunde bezeichneten Fassung einen Bestandteil des Vertragswerks.

Diese Bestimmungen ergänzen die Vertragsurkunde, die AEB IKT ewb, die AGB SIK, ein allfälliges ADV sowie die projektspezifischen Sicherheitsanforderungen. Weitergehende Anforderungen dieser Bestimmungen gelten kumulativ, soweit die gleichzeitige Erfüllung möglich ist. Ist die gleichzeitige Erfüllung nicht möglich, gehen die Vertragsurkunde beziehungsweise die ausdrücklich festgelegte Rangordnung der Vertragsbestandteile vor.

Fehlt eine solche Rangordnung, gehen die spezifischen und später vereinbarten Anforderungen den allgemeinen Bestimmungen dieser AISB vor. Die AISB gelten ergänzend, soweit sie den übrigen Vertragsbestandteilen nicht widersprechen.

Während des Beschaffungsverfahrens gelten diese Bestimmungen, soweit der Lieferant Zugang zu Informationen, Daten, Systemen, Räumlichkeiten oder sonstigen Schutzobjekten von ewb erhält oder Leistungen für ewb erbringt. Im Falle eines Vertragsschlusses gelten sie während der gesamten Vertragsdauer.

Die Bestimmungen orientieren sich insbesondere an ISO/IEC 27001:2022 und am IKT-Minimalstandard. Die gesetzlichen, regulatorischen und branchenspezifischen

Vorschriften gelten nur, soweit sie auf ewb, den Lieferanten oder die konkrete Leistung anwendbar sind. Die vertragliche Geltung dieser Bestimmungen bleibt davon unberührt.

2. Allgemeine Pflichten

2.1 Informationssicherheitsmanagement

Der Lieferant unterhält einen der Art der Leistung, dem Schutzbedarf der betroffenen Informationen und Systeme sowie den bestehenden Risiken angemessenen und dokumentierten Informationssicherheitsprozess.

Eine Zertifizierung oder die Einhaltung eines bestimmten Sicherheitsmanagementsystems ist nur geschuldet, wenn dies in der Offertanfrage, den Ausschreibungsunterlagen oder dem Vertrag ausdrücklich verlangt wird. Vom Lieferanten angegebene Zertifizierungen sind während des zugesicherten Zeitraums aufrechtzuerhalten und ewb auf Verlangen nachzuweisen.

Der Lieferant stellt sicher, dass die für die Leistungserbringung eingesetzten Mitarbeitenden und Sublieferanten die für sie relevanten Sicherheitsanforderungen einhalten. Weitergehende Genehmigungs-, Auswahl-, Kontroll- und Haftungsbestimmungen der übrigen Vertragsbestandteile bleiben vorbehalten.

2.2 Datenschutz und Vertraulichkeit

Der Lieferant hält bei der Bearbeitung von Personendaten die auf die konkrete Bearbeitung anwendbaren datenschutzrechtlichen Vorschriften sowie die einschlägigen Bestimmungen des Vertragswerks ein.

Bearbeitet der Lieferant Personendaten im Auftrag von ewb, ist vor Beginn der Bearbeitung ein ADV abzuschliessen.

Die Vertraulichkeitspflichten richten sich nach den einschlägigen Bestimmungen des Vertragswerks. Eine separate Vertraulichkeitserklärung ist abzuschliessen, wenn ewb dies aufgrund des Schutzbedarfs verlangt oder noch keine mindestens gleichwertige Vertraulichkeitsverpflichtung besteht.

2.3 Offenlegung und Auditrecht

Der Lieferant stellt ewb auf Verlangen die zur Beurteilung seiner Informationssicherheit erforderlichen Nachweise, insbesondere Sicherheitskonzepte, Zertifikate, Prüfberichte oder Beschreibungen der getroffenen Sicherheitsmassnahmen, zur Verfügung.

Durchführung, Umfang, Vorankündigung und Kostentragung von Audits richten sich nach den einschlägigen Bestimmungen des Vertragswerks. Werden im Rahmen eines Audits wesentliche Sicherheitsmängel festgestellt, trägt der Lieferant die gesamten Kosten des Audits sowie allfälliger Nachprüfungen. Bei einem Informationssicherheitsvorfall oder einer unmittelbar drohenden Gefährdung bleiben kurzfristige Überprüfungs- und Informationsrechte von ewb vorbehalten.

Der Lieferant stellt sicher, dass die vertraglich vereinbarten Prüf- und Nachweisrechte auch gegenüber den von ihm eingesetzten Sublieferanten wahrgenommen werden können.

Stellt ewb im Rahmen eines Nachweises oder Audits eine Abweichung von diesen Bestimmungen oder den vereinbarten Sicherheitsanforderungen fest, legt der Lieferant ewb innerhalb von zehn Arbeitstagen einen nachvollziehbaren Massnahmenplan mit Verantwortlichkeiten und Terminen vor und setzt die Massnahmen innerhalb der vereinbarten Fristen um. Bei einer unmittelbar drohenden Gefährdung trifft der Lieferant unverzüglich geeignete Schutzmassnahmen und informiert ewb darüber.

3. Meldepflichten

ewb unterliegt als kritische Infrastruktur verschiedenen Meldepflichten und Fristen, bei deren Erfüllung und Einhaltung sie auf ihre Lieferanten angewiesen ist.

3.1 Informationssicherheitsvorfall und Datenschutzverletzungen

Als «Informationssicherheitsvorfall» gilt jedes tatsächliche oder hinreichend konkret drohende, absichtlich oder unbeabsichtigt ausgelöste Ereignis im Zusammenhang mit Informatikmitteln, das dazu führt, dass die Vertraulichkeit, Verfügbarkeit oder Integrität von Informationen oder die Nachvollziehbarkeit ihrer Bearbeitung beeinträchtigt ist oder beeinträchtigt werden kann.

Für ewb relevant ist ein solcher Informationssicherheitsvorfall, wenn er direkt oder indirekt die Vertraulichkeit, Verfügbarkeit, Integrität oder Nachvollziehbarkeit von ewb-Daten oder ewb-Systemen beeinträchtigt oder gefährdet. Dies gilt auch nach der Beendigung des Vertragsverhältnisses, soweit der Informationssicherheitsvorfall mit den für ewb erbrachten Leistungen, noch vorhandenen ewb-Daten oder fortbestehenden Zugriffs- oder Gefährdungsmöglichkeiten zusammenhängt. Dies gilt insbesondere, wenn die angegriffenen Informatikmittel Zugang zu Informatikmitteln von ewb haben oder wenn Anzeichen dafür bestehen, dass diese Angriffe zur Vorbereitung weiterer Cyberangriffe ausgeführt wurden oder mit Erpressung, Drohung oder Nötigung verbunden sind.

Der Lieferant meldet ewb einen solchen Informationssicherheitsvorfall unverzüglich ab Entdeckung oder begründetem Verdacht, spätestens jedoch innerhalb von vier Stunden. Die Erstmeldung darf unvollständig sein und ist laufend zu ergänzen. Sie enthält, soweit bekannt, mindestens Angaben zur Art und zum Zeitpunkt des Vorfalls, zu den betroffenen Systemen und Daten, zu den möglichen Auswirkungen, zu den bereits getroffenen Sofortmassnahmen sowie zu einer zuständigen Kontaktperson. Die Parteien tauschen sich dann laufend über Art und Ursache des Vorfalls, mögliche und tatsächliche Auswirkungen, geplante und getroffene Massnahmen aus. Der Lieferant erstellt nach Abschluss der Vorfallbearbeitung eine Ursachenanalyse und einen Abschlussbericht.

Der Lieferant nimmt im Zusammenhang mit einem ewb betreffenden Informationssicherheitsvorfall keine Kommunikation im Namen von ewb gegenüber Behörden, Medien, betroffenen Personen oder weiteren Dritten vor, soweit er hierzu nicht gesetzlich verpflichtet ist oder ewb ihn hierzu in Textform aufgefordert hat. Gesetzliche Melde- und Auskunftspflichten des Lieferanten bleiben vorbehalten: der Lieferant informiert ewb darüber unverzüglich, soweit rechtlich zulässig.

Die Meldungen sind an die von ewb in den Ausschreibungsunterlagen, der Bestellung, der Auftragsbestätigung oder dem Vertrag bezeichnete Meldestelle zu richten. ewb

kann die Kontaktdaten und technischen Meldewege jederzeit in Textform aktualisieren.

Für die Erkennung, Meldung, Eindämmung und Behebung von Schwachstellen gilt Ziffer 4.3. Bereits bestehende Gewährleistungs-, Wartungs- und Nachbesserungspflichten des Lieferanten sowie die Regelungen zur Vergütung und Kostentragung in den anwendbaren Vertragsdokumenten bleiben unberührt.

Bei Datenschutzverletzungen und sonstigen Security Incidents gelten die vorstehenden Melde-, Informations- und Mitwirkungspflichten entsprechend, sofern ewb-Personendaten sowie - Daten betroffen sind oder betroffen sein könnten. Der Lieferant unterstützt ewb rechtzeitig und angemessen bei der Erfüllung ihrer gesetzlichen Melde- und Informationspflichten.

3.2 Eingesetzte Mitarbeitende und Sublieferanten

Der Lieferant dokumentiert die Personen, die im Rahmen der Leistungserbringung Zugriff auf Systeme, Räumlichkeiten, Assets oder nicht öffentliche Informationen von ewb erhalten oder eine andere sicherheitsrelevante Funktion ausüben. Er gibt ewb die für die Zugriffs- und Sicherheitsverwaltung erforderlichen Angaben auf Verlangen bekannt.

Sicherheitsrelevante Ein- und Austritte sowie Änderungen der eingesetzten Personen sind ewb so rechtzeitig mitzuteilen, dass Zugriffs- und Zutrittsberechtigungen angepasst werden können. Der Lieferant stellt sicher, dass die zugehörigen Berechtigungen und Authentisierungsmittel unverzüglich entzogen oder angepasst werden.

Der Lieferant dokumentiert die im Zusammenhang mit der Leistungserbringung eingesetzten Sublieferanten und gibt diese ewb bekannt. Genehmigungs-, Änderungs- und Haftungsregelungen der übrigen Vertragsbestandteile, insbesondere des ADV, bleiben vorbehalten.

4. Mitwirkungspflichten

ewb hat als kritische Infrastruktur eine Sorgfaltspflicht, bei deren Erfüllung sie auch auf die Mitwirkung ihrer Lieferanten angewiesen ist.

4.1 Informationssicherheitsvorfälle und Datenschutzverletzungen

Der Lieferant gewährt ewb und den von ewb beigezogenen, zur Vertraulichkeit verpflichteten Fachpersonen Zugang zu denjenigen Analysen, Berichten, Log-Daten und sonstigen Informationen, die zur Untersuchung und Bewältigung eines ewb betreffenden Informationssicherheitsvorfalls sowie einer Datenschutzverletzung erforderlich sind.

Der Zugang ist auf den betroffenen Sachverhalt zu beschränken. Gesetzliche Geheimhaltungspflichten, der Schutz von Daten anderer Kunden und berechnete Geschäftsgeheimnisse des Lieferanten sind angemessen zu berücksichtigen, ohne die wirkungsvolle Vorfallobearbeitung zu beeinträchtigen.

Der Lieferant bewahrt die für die Untersuchung und Bewältigung eines Vorfalls relevanten Protokolle, Analysedaten, Konfigurationsstände und sonstigen Beweismittel vollständig und gegen unbefugte Veränderung geschützt während den anwendbaren gesetzlichen Aufbewahrungsfristen oder bis ewb deren Freigabe

zur Löschung erteilt. Er unterlässt Massnahmen, welche die forensische Auswertung unangemessen erschweren, soweit dies nicht zur unmittelbaren Gefahrenabwehr erforderlich ist. Die Mitwirkung und Bereitstellung von Log- und Analysedaten im Rahmen der Incident-Bewältigung erfolgt für ewb kostenlos, es sei denn, der Vorfall lag nachweislich ausschliesslich in der Sphäre von ewb.

4.2 Krisen oder Notfälle

Der Lieferant unterhält eine der Kritikalität seiner Leistungen angemessene Notfall- und Krisenorganisation. Er weist ewb deren Funktionsfähigkeit auf Verlangen in geeigneter Form nach und wirkt bei abgestimmten Notfall- und Wiederanlaufübungen mit.

Leistungsspezifische Anforderungen, insbesondere Wiederanlaufzeit, maximaler Datenverlust, Notbetriebsleistungen und Verfügbarkeit, werden in der Offertanfrage, den Ausschreibungsunterlagen, der Bestellung oder dem Vertrag festgelegt.

4.3 Schwachstellen

Der Lieferant unterhält einen dokumentierten Prozess zur fortlaufenden Erkennung, Bewertung, Priorisierung, Meldung, Eindämmung und Behebung von Schwachstellen in allen für die Leistungserbringung eingesetzten Systemen, Produkten, Komponenten und Diensten. Er berücksichtigt dabei mindestens die technische Schwere, die tatsächliche oder wahrscheinliche Ausnutzbarkeit, eine bekannte aktive Ausnutzung, die Exponiertheit sowie die mögliche Auswirkung auf ewb-Systeme, ewb-Daten und ewb-Leistungen.

Er informiert ewb unverzüglich über Schwachstellen, die sich wesentlich auf die Sicherheit von ewb-Systemen, -Informationen oder -Leistungen auswirken können, und bezeichnet geeignete Schutz- oder Behebungsmassnahmen.

Der Lieferant behebt Schwachstellen, (d.h. Schwächen oder Fehler in Informatikmitteln mit dem Potenzial, einen Cyberangriff zu ermöglichen), welche vor, während oder nach einem Cyberangriff entdeckt wurden, risikogerecht und innerhalb der vertraglich festgelegten Fristen. Fehlt eine vertragliche Frist, stellt der Lieferant ewb Security Updates oder Patches für Schwachstellen mit Kritikalität «Kritisch» (CVSS ≥ 9.0) binnen maximal 5 Arbeitstagen (bzw. Workarounds binnen 2 Arbeitstagen) und für Schwachstellen mit Kritikalität «Hoch» (CVSS 7.0–8.9) binnen 30 Arbeitstagen kostenlos zur Verfügung.

Fristen, Umfang und Kosten der Bereitstellung und Implementierung von Updates, Patches und sonstigen Behebungsmassnahmen richten sich nach den einschlägigen Bestimmungen des Vertragswerks. Der Lieferant darf die Erfüllung bereits bestehender Gewährleistungs-, Pflege- oder Sicherheitsverpflichtungen nicht von einer zusätzlichen Vergütung abhängig machen.

4.4 Kryptographische Verfahren

Werden im Rahmen der Vertragserbringung durch den Lieferanten kryptographische Verfahren eingesetzt, sind diese zu dokumentieren. Der Lieferant stellt sicher, dass die eingesetzten kryptographischen Verfahren dem aktuellen Stand der Technik entsprechen. Geeignete Verfahren sind vor allem solche, welche durch unabhängige Dritte (insb. das deutsche BSI oder das amerikanische NIST) als sicher eingestuft

sind. Abweichungen davon sind durch den Lieferanten gegenüber ewb unverzüglich auszuweisen.

4.5 Nutzung von ewb Assets

Der Lieferant schützt die ihm überlassenen Arbeits-, Zutritts- und Authentisierungsmitel vor Verlust, Beschädigung und unbefugter Verwendung. Verlust, Missbrauch oder Beschädigung sind ewb unverzüglich zu melden.

Die Rückgabe richtet sich nach den Fristen und Modalitäten des Vertragswerks. Fehlt eine entsprechende Regelung, sind die Mittel nach Wegfall des Verwendungszwecks unverzüglich zurückzugeben.

5. Sorgfaltspflichten

5.1 Sicherstellung der Informationssicherheit

Der Lieferant verpflichtet sich, seine Informatikmittel (d.h. Mittel der Informations- und Kommunikationstechnik, namentlich Anwendungen, Informationssysteme und Datensammlungen sowie Einrichtungen, Produkte und Dienste, die zur elektronischen Verarbeitung von Informationen dienen) mit potenzieller Berührung zum vorliegenden Vertragsgegenstand mit ewb kontinuierlich nach dem jeweils aktuellen Stand der Technik vor Cyberangriffen dem Risiko angemessen zu schützen.

5.2 Umgang mit ewb Assets und Daten

Der Lieferant behandelt Informationen und Daten von ewb entsprechend ihrem Schutzbedarf und hält die auf die konkrete Leistung anwendbaren gesetzlichen, regulatorischen, vertraglichen und projektspezifischen Sicherheitsanforderungen ein. Weitergehende Anforderungen des ADV und anderer Vertragsbestandteile bleiben vorbehalten.

Soweit der Lieferant für die Verfügbarkeit oder Wiederherstellung von ewb-Daten verantwortlich ist, unterhält er dokumentierte Backup- und Restore-Verfahren, die dem Schutzbedarf, den vereinbarten Wiederanlaufzeiten und dem maximal zulässigen Datenverlust entsprechen. Er testet die Wiederherstellung mindestens jährlich sowie nach wesentlichen Änderungen und dokumentiert die Ergebnisse und festgestellte Mängel. Er stellt ewb den Testbericht unaufgefordert bzw. auf erstes Verlangen zur Verfügung. Die Sicherungen sind gegen unbefugte Veränderung, Verlust und unbefugten Zugriff angemessen zu schützen.

Der Lieferant muss Änderungen an informationsverarbeitenden Systemen über einen Änderungsprozess dokumentieren und freigeben. Dabei müssen mögliche negative Auswirkungen (Risiken) auf die Informationssicherheit betrachtet werden. Zur Aktualisierung der Software muss ein regelmässiges / angemessenes Update-Verfahren verfolgt werden.

Der Lieferant muss technische und prozessuale Schutzmassnahmen zur Verhinderung von Abfluss von ewb-Daten («Data Leakage») implementieren. Dies kann z.B. durch Zugriffskontrollen sichergestellt werden.

Der Lieferant schützt Informationen und Daten von ewb jederzeit vor unbefugtem Zugriff durch Dritte innerhalb und ausserhalb seiner Infrastruktur: dies gilt für elektronische sowie für physisch gespeicherte Informationen und Daten.

Bei Beendigung der Leistungserbringung führt der Lieferant die Rückgabe, Übertragung, Aufbewahrung, Sperrung und Löschung von Informationen und Daten gemäss den einschlägigen Bestimmungen des Vertragswerks durch.

Er stellt zusätzlich sicher, dass nicht mehr erforderliche Zugriffe auf ewb-Systeme deaktiviert, überlassene Authentisierungsmittel zurückgegeben und die durchgeführten Massnahmen nachvollziehbar dokumentiert werden.

5.3 Schulung und Sensibilisierung

Der Lieferant verfolgt die Weiterentwicklungen in Themen der Informationssicherheit kontinuierlich und stellt sicher, dass seine Mitarbeitenden entsprechend ausgebildet, geschult und sensibilisiert sind. Dies gilt insbesondere für die Gegenstände der Zusammenarbeit mit ewb und deren sicherheitsrelevanten Eigenschaften.

5.4 Zugriffe, Zutritte und Fernzugriffe

Der Lieferant muss den Zugriff auf gespeicherte Daten über entsprechende Berechtigungen schützen. Mitarbeiter dürfen nur Zugriff auf Daten erhalten, die sie für ihre Arbeit benötigen (Need-To-Know-Prinzip). Der Lieferant muss die vergebenen Berechtigungen periodisch überprüfen, und bei Nicht-Gebrauch von Berechtigungen müssen diese zeitnah gelöscht werden. Alle Berechtigungen müssen bei Austritt des Mitarbeitenden umgehend entzogen werden. Jeder Fernzugriff (Remote Access) auf Systeme von ewb oder Systeme, die ewb-Daten verarbeiten, muss zwingend über Multi-Faktor-Authentisierung (MFA) und verschlüsselte Kanäle erfolgen.

Der Lieferant setzt in sicherheitsrelevanten Funktionen nur sorgfältig ausgewählte und geeignete Personen ein. Weitergehende Personensicherheitsprüfungen dürfen nur verlangt oder durchgeführt werden, soweit dies aufgrund des Schutzbedarfs erforderlich, gesetzlich zulässig und in der Offertanfrage, den Ausschreibungsunterlagen oder dem Vertrag vorgesehen ist.

ewb kann im gesetzlich zulässigen Umfang geeignete Nachweise verlangen. Nicht erforderliche Personendaten oder vollständige Registerauszüge sind ewb nicht offenzulegen.

6. Weitere Pflichten je nach Anwendungsbereich

Je nach Art und Schutzbedarf der Leistung können insbesondere Anforderungen zur sicheren Softwareentwicklung, Systemsicherheit, Nutzung von Cloud-Diensten, Zugriffskontrolle und zu Fernzugriffen zur Anwendung kommen.

Die anwendbaren Anforderungen und Arbeitsanweisungen werden in der Offertanfrage, den Ausschreibungsunterlagen, der Bestellung oder dem Vertrag unter Angabe von Titel, Version und Datum bezeichnet und dem Lieferanten vor Abgabe seines verbindlichen Angebots zugänglich gemacht.

Spätere Änderungen solcher Anforderungen werden nur nach Massgabe des anwendbaren vertraglichen Änderungsverfahrens verbindlich. Zwingende gesetzliche oder regulatorische Anforderungen bleiben vorbehalten.

7. Freigabe durch
Energie Wasser Bern

A handwritten signature in blue ink, appearing to be 'M. Mattes', with a large loop at the start and a horizontal stroke at the end.

Marion Mattes
Chief Information Officer

A handwritten signature in black ink, appearing to be 'A. Sebai', with a large 'A' and a horizontal stroke at the end.

Anis Sebai
Chief Information Security Officer