Information security requirements for Suppliers

Anforderungen an Informationssicherheit für Lieferanten

BAUMANN

1. General

This document describes the minimum requirements for information security that all contractors of the BAUMANN Group must comply with. This primarily concerns ensuring the confidentiality, integrity, and availability of information. In addition to these protection objectives, the contractor is also obliged to comply with the requirements regarding prototype protection. For this reason, our contractors and service providers should establish and maintain a functioning information security management system (ISMS).

Regulations governing cooperation and communication between the client and the contractor are essential for maintaining information security, especially if confidential company information is to be shared in the course of the business relationship.

2. Rules on information security

Protection requirements and documentation obligations
BAUMANN distinguishes between three levels of requirements based on the protection needs of the information shared with suppliers. BAUMANN defines the protection needs for each supplier category or supplier and requires suppliers to meet the respective protection requirements in accordance with the following table.
The contractor undertakes to implement the protection requirements. All information related in any way to BAUMANN must comply with the protection requirements defined by BAUMANN.

Classification of shared information	Minimum requirements
1 No protection required	No security requirements
2 Normal protection required	Valid ISO 27001 certificate, ISO/IEC 22237, "TISAX label," NIS2, or similar (to be verified by CISO) or Completion of the "Supplier self-assessment on information security" (every 3 years)
3 High protection requirements	Valid ISO 27001 certificate, ISO/IEC 22237, "TISAX label," NIS2, or similar (to be checked by CISO) or On-site audit every 2 years (conducted by CISO)

Exchange of information
When information is exchanged, it must be transmitted in encrypted form in accordance with its protection requirements if this is necessary to meet the protection requirements. Unauthorized persons must be prevented from viewing, modifying, or deleting information. When information is shared verbally (e.g. on site or over the phone), care must be taken to ensure that it cannot be overheard by unauthorized persons.

Work equipment
The contractor documents the issuance of work equipment and regulates its proper return. This also includes work equipment belonging to customers or clients, such as access tokens, notebooks, etc. Only licensed hardware and

1. Allgemeines

Dieses Dokument beschreibt die Mindestanforderungen zur Informationssicherheit, die alle Auftragnehmer der BAUMANN Group einhalten müssen. Dies betrifft vor allem die Erhaltung von Vertraulichkeit, Integrität und Verfügbarkeit von Information. Neben der Einhaltung dieser Schutzziele ist der Auftragnehmer verpflichtet sich an die Anforderungen zur Einhaltung des Prototypenschutzes zu halten. Aus diesem Grund sollten unsere Auftragnehmer und Dienstleister ein funktionierendes Informationssicherheitsmanagementsystem (ISMS) einrichten und unterhalten.

Für die Wahrung der Informationssicherheit sind Regelungen zur Zusammenarbeit und Kommunikation zwischen Auftraggeber und Auftragnehmer unerlässlich, insbesondere wenn firmenvertrauliche Informationen im Verlauf der Geschäftsbeziehung geteilt werden sollen.

2. Regeln zur Informationssicherheit

Schutzanforderungen und Nachweispflichten
BAUMANN unterscheidet drei Stufen von Anforderungen anhand des Schutzbedarfs der mit den Lieferanten geteilten Informationen. BAUMANN definiert den Schutzbedarf pro Lieferantenkategorie, respektive Lieferant, und fordert die jeweiligen Schutzanforderungen gemäss der nachfolgenden Tabelle bei den Lieferanten ein.
Der Auftragnehmer verpflichtet sich, die Schutzanforderungen umzusetzen. Für alle Informationen, die in irgendeiner Form mit BAUMANN zusammenhängen, müssen die von BAUMANN definierten Schutzanforderungen eingehalten werden.

Klassifizierung der geteilten Informationen	Mindestanforderungen
1 Kein Schutzbedarf	Keine Schutzanforderungen
2 Normaler Schutzbedarf	Gültiges ISO 27001-Zertifikat, ISO/IEC 22237, «TISAX-Label», NIS2 oder ähnliches (zu prüfen durch CISO) oder Ausfüllen der «Lieferantenselbstauskunft zur Informationssicherheit» (Alle 3 Jahre)
3 Hoher Schutzbedarf	Gültiges ISO 27001-Zertifikat, ISO/IEC 22237, «TISAX-Label», NIS2 oder ähnliches (zu prüfen durch CISO) oder Vor-Ort-Audit alle 2 Jahre (durchgeführt durch CISO)

Austausch von Informationen
Wenn Informationen ausgetauscht werden, müssen diese gemäss ihrer Schutzanforderungen verschlüsselt übertragen werden, wenn dies der Schutzbedarf erfordert. Unbefugte müssen daran gehindert werden Informationen einzusehen, zu ändern oder zu löschen. Wenn Informationen auf mündlichen Wegen geteilt werden, ist darauf zu achten, dass sie nicht von unbefugten Personen abgehört werden können.

Arbeitsmittel
Der Auftragnehmer dokumentiert die Ausgabe von Arbeitsmitteln und regelt die ordnungsgemässe Rückgabe. Dies umfasst auch Arbeitsmittel von Kunden oder

software is used by the contractor to perform its tasks.	Auftraggebern wie z.B. Zugangstoken, Notebooks, etc. Zur Aufgabenerfüllung wird beim Auftragnehmer ausschliesslich lizensierte Hard- und Software eingesetzt.
Physical transport of mobile devices All data carriers, data, or data storage devices containing information from BAUMANN must be protected against unauthorized access, misuse, or falsification during transport. All necessary precautions must be taken. Data storage devices must be transported concealed. Laptops on which BAUMANN information is stored must be secured and stowed during transport in such a way that they are not openly visible – in particular, they must not be left unattended and visible in parked vehicles (e.g., on the front seat). In addition, when using them in public, care must be taken to ensure that no information can be read on the screen.	**Physischer Transport von mobilen Geräten** Alle Datenträger, Daten oder Datenspeichergeräte, die Informationen von BAUMANN enthalten, müssen während des Transports vor unbefugtem Zugriff, Missbrauch oder Verfälschung geschützt werden. Dabei müssen alle notwendigen Vorsichtsmaßnahmen getroffen werden. Datenspeichergeräte müssen verdeckt transportiert werden. Laptops, auf denen Informationen von BAUMANN gespeichert sind, müssen beim Transport so gesichert und verstaut werden, dass sie nicht offen sichtbar sind – insbesondere dürfen sie nicht unbeaufsichtigt und sichtbar in geparkten Fahrzeugen zurückgelassen werden (z. B. auf dem Vordersitz). Ausserdem ist bei der Verwendung in der Öffentlichkeit darauf zu achten darauf geachtet werden, dass keine Informationen auf dem Bildschirm gelesen werden können.
Data carrier control The contractor has implemented measures to prevent unauthorized reading, copying, modification, or deletion of data carriers (e.g., in notebooks, servers, external hard drives, USB sticks, etc.). Furthermore, rules and procedures are in place for the handling, disposal, and transport of data carriers.	**Datenträgerkontrolle** Beim Auftragnehmer sind Massnahmen umgesetzt, die das unbefugte Lesen, Kopieren, Verändern oder Löschen von Datenträgern (z.B. in Notebooks, Servern, externen Festplatten, USB-Sticks, etc.) verhindern. Des Weiteren gibt es Regeln und Verfahren zum Umgang, Entsorgung und Transport.
Mobile devices and remote working The contractor regulates the use of mobile devices and ensures compliance with security measures. Measures to protect information accessed via remote working have been implemented.	**Mobilgeräte und Remotearbeit** Beim Auftragnehmer ist die Nutzung von mobilen Endgeräten geregelt und die Einhaltung von Sicherheitsmassnahmen sichergestellt. Massnahmen zum Schutz von Information, auf die per Remotearbeit zugegriffen wird, sind umgesetzt.
Access and access control The contractor has a formal, documented process for registering, deregistering, and assigning user access. Access rights are assigned according to the need-to-know principle. Privileged rights are granted on a restrictive basis. It is ensured that users can only access the information covered by their access authorization. It is ensured that the login procedures are secure and state-of-the-art.	**Zugangs- und Zugriffskontrolle** Beim Auftragnehmer ist die Registrierung, Deregistrierung und Zuteilung von Benutzerzugängen ein formaler Prozess und dokumentiert. Eine Zuweisung von Zugriffsrechten erfolgt nach dem Need-To-Know – Prinzip. Die Erteilung von privilegierten Rechten geschieht restriktiv. Es wird gewährleistet, dass Benutzer nur auf die von ihrer Zugangsberechtigung umfassten Informationen zugreifen können. Es ist sichergestellt, dass die Anmeldeverfahren auf sicherem Wege geschehen und dem Stand der Technik entsprechen.
Passwords The contractor's handling of passwords is defined and employees are obliged to comply with these guidelines. These include rules for storing passwords, changing passwords, and handling customer passwords.	**Passwörter** Der Umgang mit Passwörtern beim Auftragnehmer ist festgelegt und die Mitarbeiter sind zur Einhaltung dieser Vorgaben verpflichtet. Diese beinhaltet Regeln zur Aufbewahrung von Passwörtern, Passwortwechsel und den Umgang mit Kundenpasswörtern.
Physical security Appropriate protective measures are implemented by the contractor for areas where sensitive or critical information is located. Access is regulated and it is ensured that only authorized persons can enter these areas.	**Physische Sicherheit** Für Bereiche, in denen sich sensible oder kritische Information befindet, sind beim Auftragnehmer angemessene Schutzmassnahmen umgesetzt. Der Zutritt ist geregelt und sichergestellt, dass nur berechtigte Personen in diese Bereiche gelangen können.
Device lock The contractor's systems (e.g., workstations, notebooks, mobile phones, smartphones, etc.) are equipped with automatic mechanisms that automatically lock after no more than 5 minutes of inactivity. Furthermore, users are required to lock the system after use.	**Gerätesperre** In Systemen des Auftragnehmers (z.B. Workstations, Notebooks, Mobiltelefone, Smartphones, etc), sind Automatismen eingerichtet, die die Nutzung des Gerätes nach einer Inaktivität von spätestens 5 Minuten sperrt. Des Weiteren sind die Benutzer verpflichtet, das System nach der Nutzung zu sperren.

Measures against malware The contractor shall ensure that the systems it operates are protected against malware and that anti-malware signatures are always kept up to date.	**Massnahmen gegen Schadsoftware** Der Auftragnehmer stellt sicher, dass die von ihm betriebenen Systeme gegen Schadsoftware geschützt sind und Anti-Malware-Signaturen stets aktuell gehalten werden.
Data backup The contractor shall ensure that information is continuously protected against loss and can be restored within a reasonable timeframe.	**Datensicherung** Der Auftragnehmer stellt sicher, dass Informationen jederzeit gegen Verlust geschützt sind und in einem angemessenen Zeitraum wiederhergestellt werden können.
Software updates The contractor shall ensure that the software packages used for operating systems and applications originate from secure sources. Regular updates of systems and applications shall be ensured via a controlled update process.	**Aktualisierung von Software** Der Auftragnehmer stellt sicher, dass die für Betriebssysteme und Anwendungen eingesetzten Softwarepakete aus sicheren Quellen stammt. Die regelmässige Aktualisierung der Systeme und Anwendungen wird über einen gesteuerten Updateprozess gewährleistet.
Publicly accessible application services Application services operated by the contractor on public networks on which information belonging to the client or its customers is transmitted, stored, or processed are subject to constant monitoring by the contractor. Operation, update management, measures against malware, vulnerability management, and data backup are controlled.	**Öffentlich erreichbare Anwendungsdienste** Vom Auftragnehmer in öffentlichen Netzwerken betriebene Anwendungsdienste, auf denen Information des Auftraggebers oder dessen Kunden übermittelt, gespeichert oder verarbeitet werden, unterliegen einer ständigen Kontrolle des Auftragnehmers. Der Betrieb, die Updateverwaltung, Massnahmen gegen Schadsoftware, Schwachstellenmanagement sowie Datensicherung sind gesteuert.
Guideline for secure development When developing systems or applications, the contractor must ensure that appropriate information security controls are implemented in line with current best practices. The specifications and guidelines of the client and its customers must be observed.	**Richtlinie für sichere Entwicklung** Bei der Entwicklung von Systemen oder Anwendungen hat der Auftragnehmer darauf zu achten, dass Informationssicherheitsaspekte gemäss dem Stand der Technik berücksichtigt werden. Die Vorgaben und Richtlinien des Auftraggebers sowie dessen Kunden sind zu beachten.
Rules for access to the client's or its customers' systems Any attempt to guess passwords or to circumvent system restrictions is strictly prohibited. Activities that place a strain on the network beyond the scope of normal use (network scans, vulnerability scans, broadcasts) must be agreed with the client in advance and require the client's approval.	**Regeln bei Zugriffsmöglichkeiten auf Systeme des Auftraggebers oder dessen Kunden** Das Ausprobieren von Passwörtern oder der Versuch der Umgehung von Beschränkungen ist nicht gestattet. Tätigkeiten, die das Netzwerk über den Rahmen der üblichen Nutzung belasten (Netzwerk-Scans, Vulnerability-Scans, Broadcast) sind mit dem Auftraggeber im Vorfeld abzustimmen und bedürfen der Genehmigung des Auftraggebers.
Deletion of information At the client's request, all information related to the project or order must be deleted. The contractor must provide proof of proper destruction.	**Löschung von Information** Auf Verlangen des Auftraggebers sind alle Informationen, die mit dem Projekt oder Auftrag in Zusammenhang stehen, zu löschen. Der Nachweis der ordnungsgemässen Vernichtung ist durch den Auftragnehmer zu erbringen.
Dealing with information security incidents Information security incidents or any suspicion of a loss of confidential information must be reported immediately to the designated contact person (e.g. system malfunctions, data loss, illegal activities, cyberattacks).	**Umgang mit Informationssicherheitsvorfällen** Informationssicherheitsvorfälle und jeglicher Verdacht auf Verlust von vertraulichen Informationen müssen ungehend an den oben genannten Ansprechpartner gemeldet werden (z. B. Störungen, Datenverluste, rechtswidrige Handlungen, Cybercrime-Angriffe).
Compliance with information security (supply chain) When commissioning subcontractors, the contractor must ensure that the requirements imposed by BAUMANN on the contractor are also passed on to the subcontractor. This includes the conclusion of confidentiality agreements. The contractor is responsible for providing proof of compliance. The commissioning of subcontractors by the contractor requires the express written consent of BAUMANN.	**Einhaltung der Informationssicherheit (Lieferkette)** Der Auftragnehmer muss bei der Beauftragung von Subunternehmern sicherstellen, dass die Anforderungen, die BAUMANN an den Auftragnehmer stellt, ebenfalls an den Subunternehmer weitergegeben werden. Dazu gehört auch der Abschluss von Geheimhaltungsvereinbarungen. Der Nachweis der Einhaltung liegt in der Verantwortung des Auftragnehmers. Die Beauftragung von Unterauftragnehmern durch den Auftragnehmer bedarf der ausdrücklichen schriftliche Zustimmung von BAUMANN.
Right to audit with regard to information security The contractor guarantees the client the right to verify the implementation of the requirements defined here on the contractor's premises. This audit may also be carried out by third-party companies commissioned by the client for this	**Recht auf Audit in Bezug auf die Informationssicherheit** Der Auftragnehmer sichert dem Auftraggeber das Recht zu, sich von der Umsetzung der hier definierten Vorgaben in den Räumlichkeiten des Auftragnehmers zu überzeugen. Diese

purpose.

3. Contact

The central contact person for all questions regarding these regulations and all other matters relating to information security is the CISO of the BAUMANN Group:

Sebastian Müller
Email: ciso@baumann-group.com

All information security incidents must be reported to the CISO without delay.

4. Declaration of commitment

We hereby declare that we agree to fulfill the above requirements.

Company

Street No.

Zip Code, City

Name

Function

Place, Date

Signature

Auditierung kann auch von Drittunternehmen durchgeführt werden, die der Auftraggeber zu diesem Zweck beauftragt.

3. Kontakt

Zentraler Ansprechpartner für alle Fragen zu diesen Regelungen und allen weiteren Belangen zur Informationssicherheit ist der CISO der BAUMANN Group:

Sebastian Müller
E-Mail: ciso@baumann-group.com

Alle Meldungen zu Informationssicherheitsereignissen haben schnellstmöglich an den CISO zu erfolgen.

4. Verpflichtungserklärung

Wir erklären hiermit, dass wir uns zur Erfüllung der oben genannten Anforderungen verpflichten.