**Angebotsanfrage für eine Überprüfung nach NISG §17(3)**

|  |  |  |  |
| --- | --- | --- | --- |
| Organisationsdaten | | | |
| Organisationsname: | | | Gesellschaftsform: |
| Konzernzugehörigkeit: | | | Anzahl Mitarbeiter (gesamt): |
| Tätigkeit: | | | NACE: |
| Firmensitz: | | | |
| PLZ: | Ort: | Straße: | |
| Sektor/Teilsektor (lt. Netz und Informationssicherheitsverordnung Abschnitt 2) | | | |
| Sektor: | | | |
| Teilsektor: | | | |
| **Wählen Sie eine der folgenden Optionen**  NISG §17(3) ohne ISO 27001 Zertifizierung  ODER  NISG §17(3) inkl. ISO 27001 Zertifizierung  Gewünschte Sicherheitsvorkehrungen nach NISV Beilage 1   |  |  | | --- | --- | |  | gesamte Beilage lt. NISV |   ODER   |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | 1. | Governance und Risikomanagement |  |  | 7. | Physische Sicherheit | |  | 2. | Umgang mit Dienstleistern, Lieferanten und Dritten |  |  | 8. | Erkennung von Vorfällen | |  | 3. | Sicherheitsarchitektur |  |  | 9. | Bewältigung von Vorfällen | |  | 4. | Systemadministration |  |  | 10. | Betriebskontinuität | |  | 5. | Identitäts- und Zugriffsmanagement |  |  | 11. | Krisenmanagement | |  | 6. | Systemwartung und Betrieb |  |  |  |  |  |  |  |  | | --- | --- | --- | | Ja | Nein | Technische Überprüfung gewünscht? | | Ja | Nein | Regelmäßige interne Schwachstellenscans decken den gesamten NIS Scope ab? | | | | |
| Bereits zertifiziert nach:  ISO 27001  ISO 9001  ISO 14001/EMAS  andere:  gültig bis: | | | |

|  |  |
| --- | --- |
| Informationssicherheitsrelevante Daten  Sofern exakte Daten für den Geltungsbereich nicht oder nur mit erheblichem Erhebungsaufwand verfügbar sind, können auch größenordnungsmäßige Schätzungen angegeben werden. | |
| Gesamtzahl der Mitarbeiter im Geltungsbereich des wesentlichen Dienstes (Angestellte, freie Mitarbeiter, etc.): |  |
| Summe der Standorte im Geltungsbereich des wesentlichen Dienstes: |  |
| Anzahl IKT-Arbeitsplätze: |  |
| Anzahl Server (virtuell plus physisch): |  |
| Anzahl Systemadministratoren: |  |
| Anzahl interner Softwareentwickler: |  |
| Anz. Telearbeitsplätze/Remote Zugriff: |  |
| Anzahl unterschiedlicher Sicherheitszonen: |  |
| Anz. externer IT-Lieferanten/Dienstleister: (Cloud Services, Software, Hardware, Rechenzentrumsbetreiber) |  |
| Anz. geschäftskritischer Anwendungen: |  |
| Maximal tolerierte Ausfallszeit in Stunden (MTA): |  |
| Unternehmenskritische Daten allgemein: | wenige  einige  viele |
| Einsatz von Datenverschlüsselung: | ja  nein |
| e-Commerce | ja  nein |
| e-Cash: | ja  nein |
| **Spezifisch für den wesentlichen Dienst** | |
| Anzahl OT Komponenten (Stations- und Feldleittechnik) |  |
| Anzahl SCADA Systeme |  |
| Anzahl Netzwerkkomponenten (Router/Switches/Firewalls) |  |
| Anzahl unterschiedlicher physischer Sicherheitszonen: |  |
| Anz. externer IT-Lieferanten/Dienstleister mit Betriebsverantwortung: (Cloud Services, Software, Hardware, Rechenzentrumsbetreiber) |  |
| Anz. externer IT-Lieferanten/Dienstleister ohne Betriebsverantwortung: (Cloud Services, Software, Hardware, Rechenzentrumsbetreiber) |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Hauptstandort im Geltungsbereich | | | |
| PLZ: | Ort: | Straße: | Homepage: |
| Weitere Standorte des Geltungsbereiches (ohne Telearbeitsplätze) | | | |
| Tätigkeiten am **Standort 1**: | | | |
| PLZ: | Ort: | Straße: |  |
| Tätigkeiten am **Standort 2**: | | | |
| PLZ: | Ort: | Straße: |  |

|  |  |
| --- | --- |
| Summe aller Standorte im Geltungsbereich: |  |

|  |
| --- |
| Anmerkung: Weitere Standorte des Geltungsbereichs darüber hinaus können als Anhang beigelegt werden. |

|  |  |  |
| --- | --- | --- |
| Ansprechpartner (z.B.: Geschäftsführer, IT- bzw. IS-Manager, RZ-Leitung, …) | | |
| Name: | Funktion: | Tel.: |
| E-Mail: |
| Name: | Funktion: | Tel.: |
| E-Mail: |
| Name: | Funktion: | Tel.: |
| E-Mail: |

|  |
| --- |
| Audit |
| Sprache der Dokumentation:  Deutsch  Englisch  Italienisch  Sonstige: |
| Auditsprache:  Deutsch  Englisch  Italienisch  Sonstige: |
| gewünschter Auditor: |
| CIS wird für Sie ein geeignetes Auditteam zusammenstellen. Falls Sie einen Wunschauditor angeben, wird CIS versuchen, Ihren Wunsch zu berücksichtigen. |

|  |
| --- |
| Werden Prozesse ausgegliedert die Auswirkungen auf die Organisation haben können?  ja  nein Wenn JA, welche?: |

|  |  |  |
| --- | --- | --- |
| Wurden/werden Sie durch einen Berater bzgl. Sicherheitsvorkehrungen nach NISV bzw. NISG unterstützt/beraten? | | ja  nein |
| Name des Beratungsunternehmens: |  | |
| Name des Beraters: |  | |

|  |  |
| --- | --- |
| Telefonnummer für die Übermittlung eines Passwortes (SMS), sofern eine sichere (verschlüsselte) Übermittlung des Auditberichtes gewünscht ist: |  |

**Weiterführende Unterlagen, die im Falle eines Auftrages Bestandteil des Vertrages sind:**

* NISG Überprüfungen erfolgen gemäß Dokument Nr. d118   
  CIS Prüfverfahren NISV ([Download](https://www.cis-cert.com/wp-content/uploads/d118-cis-prufverfahren-nisg-1.pdf))
* Allgemeine Geschäftsbedingungen Nr. d007 ([Download](https://www.cis-cert.com/wp-content/uploads/d007-geschaeftsbedingungen-sz-1.pdf))

|  |  |  |
| --- | --- | --- |
|  |  |  |
| Ort, Datum |  | Unterschrift mit Firmenstempel |

|  |  |  |
| --- | --- | --- |
| **Bitte Formular ausfüllen, unterzeichnen und an CIS senden:** |  | **CIS** -Certification & Information Security Services GmbH |
| © CIS 13.10.2021: Nachdruck und Vervielfältigung, auch auszugsweise, nur mit schriftlicher Genehmigung der CIS. |  | **Headquarters**  1010 Wien, Salztorgasse 2/6/14  Tel.: +43 1 532 98 90 Fax: +43 1 532 98 90 89 [office@cis-cert.com](mailto:office@cis-cert.com) [www.cis-cert.com](http://www.cis-cert.com) |