IT-Sicherheitskatalog gem. § 11 Abs. 1a EnWG

Anfrage

Per Fax an: +49 3375 217459-19 oder per E-Mail an: kundendienst@deuzert.de

DeuZert® Deutsche Zertifizierung in Bildung und Wirtschaft GmbH

Hochschulring 2, 15745 Wildau

Art der Anfrage	
Firmensitz / Hauptzentrale des Unternehmens	
Unternehmen:	
Anschrift:	
Geschäftsführung:	Vorname, Name:
Telefon:	
Internet:	
Rechnungsanschrift (wenn Anschrift von oben abweichend)	
Unternehmen:	
Straße Nr.:	
PLZ Ort:	
AnsprechpartnerIn IT-Sicherheit gegenüber BNetzA gem. IT-Sicherheitskatalog, Kap. VII	
Vorname, Name:	
Funktion:	
Anschrift:	
Telefon / Fax:	/
E-Mail:	

Informationen über das Unternehmen		
Welche Arten von Energieversorgungsnetzen betreiben Sie und wollen Sie zertifizieren?		
☐ Strom	Netzbetreiber-Nr. (BNetzA)	
☐ Gas	Netzbetreiber-Nr. (BNetzA)	
In welchen Bereichen sind Ihre Kunden vertreten (z. B. Datenverarbeitung, Automobilindustrie, usw.)?		
Hat das Unternehmen bei der Einführung und Umsetzung des IT-Sicherheitskataloges die Unterstützung eines externen Beraters / Beratungsunternehmens in Anspruch genommen?		
☐ Ja	Name des Beraters und der Beratungsgesellschaft:	
☐ Nein		
Sind nicht zutreffende Anforderungen/ Ausschlüsse aus dem Anwendungsbereich vorhanden?		
☐ Ja	Welche? Bitte Risikoakzeptanzkriterien oder sonstige Ausschlüsse angeben.	
☐ Nein		
Gibt es Informationssicherheitsmanagementsystemrelevante Bereiche in Ihrem Unternehmen, die dem Auditteam aus Geheimhaltungsgründen nicht zugänglich gemacht werden können?		
☐ Ja	Welche? Bitte angeben.	
☐ Nein		

Grunddaten des Informationssicherheitsmanagementsystems (ISMS)		
Werden die Geschäftsprozesse Ihres Unternehmens rechnergestützt abgewickelt?	☐ Ja	☐ Nein
Unterliegt Ihr Unternehmen verstärkten Forderungen bzgl. des Datenschutzes (Geheimhaltung, Verwaltung personenbezogener Daten)?	☐ Ja	☐ Nein
Betreibt Ihr Unternehmen aus Gründen der Datensicherheit „getrennte“ (dedizierte) Systeme?	☐ Ja	☐ Nein
Verwaltet Ihr Unternehmen externe Daten?	☐ Ja	☐ Nein

Informationssicherheitsanforderungen (Vertraulichkeit, Integrität, Verfügbarkeit)	☐ Viele sensitive/ vertrauliche Informationen; hohes Anforderungsniveau	☐ Eine Reihe von sensitiven/ vertraulichen Informationen; mittleres Anforderungsniveau	☐ Wenig sensitive/ vertrauliche Informationen; geringes Anforderungsniveau
Anzahl kritischer Vermögenswerte bzgl. Vertraulichkeit, Integrität, Verfügbarkeit	☐ Viele kritische Vermögenswerte	☐ Eine Reihe von kritischen Vermögenswerten	☐ Wenige kritische Vermögenswerte

Anzahl Prozesse und Services	☐ Mehr als 2 komplexe Geschäftsprozesse mit vielen Schnittstellen und einbezogenen Geschäftseinheiten	☐ Bis 3 einfache Geschäftsprozesse mit wenigen Schnittstellen und einbezogenen Geschäftseinheiten	☐ Ein Hauptgeschäftsprozess mit wenigen Schnittstellen und einbezogenen Geschäftseinheiten
Geschäftsrisiko innerhalb des Anwendungsbereiches des ISMS	☐ Hohes Geschäftsrisiko	☐ Mittleres Geschäftsrisiko mit höheren regulatorischen Anforderungen	☐ Niedriges Geschäftsrisiko ohne regulatorische Anforderungen
Umfang und Vielfalt von genutzter IT-Technologie und -Umgebung	☐ Hohe Vielfalt oder Komplexität der IT-Umgebung	☐ Standardisierte IT-Umgebung mit vielfältigen IT-Plattformen, Servern, Betriebssystemen, Datenbanken & Netzwerken	☐ Hoch standardisierte IT-Umgebung mit wenig Vielfalt
Umfang des Outsourcings an externe Dienstleister innerhalb des Anwendungsbereiches des ISMS	☐ Hohe Abhängigkeit von Outsorcing oder Lieferanten mit hohem Einfluss auf wichtige Geschäftsaktivitäten	☐ Teilweises Outsorcing	☐ Kein Outcourcing und geringe Abhängigkeit von Lieferanten oder gut etabliertes bzw. überwachtes Outsorcing mit zertifizierten ISMS beim Lieferanten
Umfang der Systementwicklung	☐ Umfangreiche interne Software-Entwicklung in verschiedenen laufenden Projekten für wichtige Geschäftsanwendungen	☐ Systementwicklung unter Nutzung standardisierter Software-Plattformen mit komplexer Konfiguration; kundenspezifische Softwarelösungen	☐ Keine Inhouse-Systementwicklung mit Nutzung standardisierter Software-Plattformen
Anzahl der Notfallwiederherstellungsstandorte (Disaster recovery sites)	☐ Hohe Anforderung (24/7) mit verschiedenen Notfallwiederherstellungsstandorten und Datencentern	☐ Mittlere Anforderung und max. 1 Notfallwiederherstellungsstandort	☐ Keine Anforderung und max. 1 Notfallwiederherstellungsstandort

Anzahl aller Mitarbeitenden (**Vollzeitäquivalent**) im Anwendungsbereich des IT-Sicherheitskataloges:	
… davon Anzahl Mitarbeitende mit identischen Tätigkeiten, ...	
➔ davon Mitarbeitende mit reinem Informationslesezugriff	
➔ davon Mitarbeitende ohne Zugang zu informationsverarbeitenden Einrichtungen	
➔ davon Mitarbeitende mit einem spezifisch, nachweislich eingeschränkten Zugang zu informationsverarbeitenden Einrichtungen	
➔ davon Mitarbeitende mit strengen Beschränkungen für die Weitergabe von Informationen, z.B. und nicht ausschließlich Verbot des Mitbringens von persönlichen Gegenständen und Geräten in den Arbeitsbereich	

Anzahl aller Mitarbeitenden	☐ ≥ 1.000	☐ ≥ 200	☐ < 200
Anzahl der Mitarbeitenden, die die IT-Systeme pflegen/ administrieren	☐ ≥ 100	☐ ≥ 20	☐ < 20
Anzahl der Betriebsstätten	☐ ≥ 5	☐ 2 bis 4	☐ 1

Daten für die Sparte Strom			
Anzahl der Mitarbeitenden in Leitstellen	☐ ≥ 30	☐ 10 bis 29	☐ < 10
Anzahl der Endverbraucher	☐ ≥ 100.000	☐ 10.000 bis 99.999	☐ < 10.000
Anzahl der elektronisch ausgelesenen Mess-punkte	☐ ≥ 100.000	☐ 10.000 bis 99.999	☐ < 10.000
Anzahl Zählerfernaus-lesung	☐ > 20	☐ 5 bis 20	☐ < 5
Anzahl Umspannwerke	☐ > 25	☐ 10 bis 25	☐ < 10
Anzahl Trafo-Stationen	☐ ≥ 1.000	☐ 100 bis 999	☐ < 100
Werden Betriebsaufgaben extern durchgeführt?			
☐ Ja	Welche Aufgaben? *Bitte kurz beschreiben.*		
☐ Nein			
Sind Sie Stromnetzbetreiber?			
☐ Ja			
☐ Nein			
Strombereitstellung in MW	☐ ≥ 1.000	☐ 200 bis 999	☐ < 200
Daten für die Sparte Gas			
Anzahl der Abnehmer	☐ ≥ 100.000	☐ 10.000 bis 99.999	☐ < 10.000
Anzahl der Großabneh-mer (Industrie u. a.)	☐ ≥ 500	☐ 50 bis 499	☐ < 50
Anzahl Verdichterstа-tionen	☐ ≥ 6	☐ < 6	☐ 0
Anzahl Gasdruckregel-anlagen	☐ ≥ 1.000	☐ 100 bis 999	☐ < 100

Dauerhaft besetzte Betriebsstätten			
Lfd. Nr.	Bezeichnung, Adresse	Mitarbeitende im Scope (VZÄ)	Art der Fernwirktechnik / Netztechnik
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

<u>Nicht</u> dauerhaft besetzte Betriebsstätten			
Bezeichnung/ Gruppierung	Art der Fernwirktechnik	Anzahl	Besonderheiten

Weitere Informationen über die Betriebsstätten Ihres Unternehmen	
Wie viele **Betriebsstätten** sollen insgesamt zertifiziert werden? *Bitte pro Betriebsstätte unser Formular „Anfrage / Angaben zur Betriebsstätte“ (WP04 K F01a) ausfüllen.*	

Eine **Verbundzertifizierung**[1] ist nur möglich, wenn folgende Punkte zutreffen:	
☐	Die Organisation wendet ein einziges Informationssicherheitsmanagement-system für alle Betriebsstätten an.
☐	Die Organisation weist eine Zentrale als Teil der Organisation auf (nicht notwendigerweise der Hauptsitz der Organisation; nicht unbedingt eine einzelne Betriebsstätte).
☐	Die Zentrale hat die organisatorische Befugnis, das Informationssicherheitsmanagementsystem zu definieren, einzuführen und zu pflegen.
☐	Das Informationssicherheitsmanagementsystem unterliegt einer zentralen Überprüfung durch die oberste Leitung der Organisation.
☐	Alle Betriebsstätten unterliegen dem internen Auditprogramm der Organisation.
☐	Die Zentrale stellt sicher, dass Daten von allen Betriebsstätten erhoben und analysiert werden. Sie kann nachweisen, dass sie in dieser Hinsicht die Befugnis und Fähigkeit zur Einleitung organisatorischer Änderungen u.a. zu Folgendem besitzt: • Managementsystemdokumentation und dessen Veränderungen, • Managementbewertung, • Behandlung von Beschwerden, • Bewertung von Korrekturmaßnahmen, • Planung interner Audits mit Bewertung der Ergebnisse sowie • Berücksichtigung/ Einhaltung gesetzlicher/ behördlicher Anforderungen in Bezug auf IT-Sicherheitskatalog gem. § 11 Abs. 1a EnWG.

Falls Änderung des Geltungsbereiches einer bestehenden Zertifizierung			
Zertifikat-Registrier-Nr.:		Ausstellungsdatum:	
Bitte beschreiben Sie die Änderung [2]:			

1 Zertifizierung einer Organisation mit einem Informationssicherheitsmanagementsystem an mehreren Betriebsstätten.
2 Handelt es sich um eine **Erweiterung des Anwendungsbereiches**, machen Sie bitte zu folgenden Faktoren dezidiert Angaben:
a) der Art der Erweiterung;
b) der Tätigkeit(en) der aktuellen Zertifizierung in Bezug auf die Erweiterung;
c) der Anzahl der Betriebsstätten, an denen die Tätigkeit(en) verrichtet wird/werden;
d) der mit der/den Tätigkeiten(en) verbundenen Informationssicherheitsrisiken;
e) der Anzahl der für die Erweiterung relevanten Maßnahmen/ Controls aus Anhang A der ISO/IEC 27001:2022;
f) der Anzahl der Mitarbeitenden im neuen Anwendungsbereich; und
g) Ihr Zeitaufwand für die Überprüfung der Integration des erweiterten Anwendungsbereichs in das ISMS (interne Audits etc.).

Weitere, abschließende Angaben	
Gewünschter Audittermin (KW Jahr):	
Ort, Datum	
Anfragender: (Titel) Vor- und Nachname im Klartext:	

Vielen Dank für Ihre Mühe.