Bundesamt
für Sicherheit in der
Informationstechnik

Allianz für
Cyber-Sicherheit

Zusatzformular INSI und KRITIS

für Institutionen im besonderen staatlichen Interesse und Betreiber Kritischer Infrastrukturen

Die Allianz für Cyber-Sicherheit bietet für teilnehmende Institutionen bei denen es sich um „Institutionen im besonderen staatlichen Interesse“ (INSI) handelt, zusätzliche Angebote und einen erweiterten, vertraulichen Informationspool an.

Zudem können sich Institutionen, bei denen es sich um Kritische Infrastrukturen handelt, ohne großen Mehraufwand unter Punkt 2 gleichzeitig für eine Teilnahme am UP KRITIS anmelden.

Um in den Teilnehmerkreis der INSI aufgenommen zu werden und bei Interesse, am UP KRITIS teilzunehmen, senden Sie uns bitte dieses Formular ausgefüllt und unterschrieben zur Prüfung zu bzw. legen Sie es Ihrer Interessenbekundung zur Teilnahme bei.

1 Begründung zur Aufnahme in den Teilnehmerkreis der INSI

Die Aufnahme in den Teilnehmerkreis der INSI erfolgt nach Prüfung der unten angegebenen Kriterien, sofern die Institution alle notwendigen Voraussetzungen erfüllt und bereits Teilnehmer der Allianz für Cyber-Sicherheit ist oder die vorliegende Interessenbekundung bereits erfolgreich geprüft wurde. Ein Rechtsanspruch zur Aufnahme besteht nicht.

1.1 Angaben zur Institution

Bitte geben Sie hier die Basisdaten Ihrer Institution an. Felder mit Sternchen **(*)** sind Pflichtangaben.

Name der Institution *	

1.2 Begründung

Bitte kreuzen Sie zutreffende Möglichkeiten an bzw. begründen Sie nachvollziehbar.

☐ Die Institution ist in der Geheimschutzbetreuung durch das BMWi. Die Registrierungsnummer gemäß Sicherheitsüberprüfungsgesetz[1] lautet:

Registrierungsnummer	

☐ Die Institution hat eine tragende wirtschaftliche Rolle in einer Region oder in Deutschland und beschäftigt zusätzlich mindestens 5.000 Mitarbeiter in Deutschland.

☐ Ein Cyber-Angriff auf die IT-Systeme der Institution kann zu einer Großgefahrenlage der öffentlichen Sicherheit, der Menschen oder der Umwelt führen. (z.B. Gefahr für Leib und Leben)

☐ Sonstige Institution im besonderen staatlichen Interesse. Begründung:

Begründung	

1 Sicherheitsüberprüfungsgesetz: http://www.gesetze-im-internet.de/s_g/index.html

☐ Die Institution gehört als Betreiber einer Branche an, die den KRITIS-Sektoren[2] zugeordnet ist, und besitzt dort einen signifikanten Versorgungsauftrag.

KRITIS-Branche			
	Energie ☐ Elektrizität ☐ Gas ☐ Mineralöl **Ernährung** ☐ Ernährungswirtschaft ☐ Lebensmittelhandel **Finanz & Versicherungswesen** ☐ Banken ☐ Börsen ☐ Versicherungen ☐ Finanzdienstleister	**Gesundheit** ☐ Medizinische Versorgung ☐ Arzneimittel und Impfstoffe ☐ Labore **Informations- & Telekommunikationstechnik** ☐ Telekommunikation ☐ Informationstechnik **Medien & Kultur** ☐ Rundfunk und Presse ☐ Kulturgut ☐ Symbolträchtige Bauwerke	**Transport & Verkehr** ☐ Luftfahrt ☐ Seeschifffahrt ☐ Binnenschifffahrt ☐ Straßenverkehr ☐ Logistik **Staat & Verwaltung** ☐ Behörde **Wasser** ☐ Wasserversorgung ☐ Abwasserbeseitigung

1.3 Notfallkontakt für Cyber-Sicherheit in der Organisation

Institutionen aus dem Teilnehmerkreis der INSI können durch das BSI in einen Verteiler für Warnmeldungen aufgenommen werden. Um in diesen Verteiler aufgenommen zu werden, geben Sie bitte hier einen Notfallkontakt für Ihre Institution an.

Gegebenenfalls kann das BSI diesen Kontakt auch im Rahmen der Vorfallsbearbeitung zur Kontaktaufnahme nutzen, z.B. wenn dem BSI Informationen bekannt werden, die Ihre Institution direkt oder indirekt betreffen.

Organisationseinheit z.B. Computer Emergency Response Team (CERT), Corporate IT-Security, etc.	
E-Mail	
Telefon	
Telefon (alternativ)	
Fax	

Hinweis: Die über den Verteiler für Warnmeldungen versandten Informationen dienen ausschließlich der Ergänzung anderweitig verfügbarer Informationsangebote und ersetzen nicht ggf. kommerzielle Angebote von CERTs und Sicherheitsdienstleistern. Der Versand von Warnmeldungen erfolgt nur in besonders relevanten Fällen nach freier Entscheidung durch das BSI, ein Anspruch auf Vollständigkeit besteht nicht.

2 Zusätzliche Anmeldung beim UP KRITIS

Der UP KRITIS ist eine öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen (KRITIS), deren Verbänden und den zuständigen staatlichen Stellen. Der UP KRITIS adressiert acht der neun Sektoren Kritischer Infrastrukturen (ohne Staat und Verwaltung).

Ziel ist die Versorgung der Bevölkerung mit wichtigen, teils lebenswichtigen Gütern und Dienstleistungen (kritischen Dienstleistungen) sicherzustellen sowie erhebliche Störungen der öffentlichen Sicherheit oder anderer dramatische Folgen zu vermeiden. Aufgrund der Bedeutung der Informationstechnik für kritische Prozesse bildet dabei die IT in den kritischen Prozessen den Schwerpunkt der Arbeiten.

Die am UP KRITIS beteiligten Organisationen arbeiten auf Basis gegenseitigen Vertrauens zusammen. Sie tauschen sich untereinander aus und lernen voneinander im Hinblick auf den Schutz Kritischer Infrastrukturen. Gemeinsam kommen alle Beteiligten so zu besseren Lösungen.

2 Sektoreinteilung der Kritischen Infrastrukturen: http://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/Sektoren/sektoren_node.de

2.1 Ansprechpartner

Der Ansprechpartner der Interessenbekundung für die Allianz für Cyber-Sicherheit soll für den UP KRITIS:

☐ als Ansprechpartner gelten.

☐ als IT/IT-Sicherheitskontakt gelten.

2.2 Ansprechpartner bzw. IT-Kontakt

Je nachdem, welcher Kontakt in 2.1 als Ansprechpartner gewählt wurde, wird hier der fehlende weitere Kontakt abgefragt. Felder mit Sternchen **(*)** sind Pflichtangaben.

Anrede	**Vorname ***	**Nachname ***

Funktion *	
Anschrift *	
E-Mail *	
Telefon *	
Fax	

2.3 Angaben zum Kontakt im Bereich BCM oder Krisenmanagement

Felder mit Sternchen **(*)** sind Pflichtangaben.

Anrede	**Vorname ***	**Nachname ***

Funktion *	
Anschrift *	
E-Mail *	
Telefon *	
Fax	

3 Einverständniserklärung

Hiermit erbitte ich für meine Institution und alle ggf. bereits zusätzlich registrierten Personen meiner Institution die Zugangsberechtigung für den erweiterten, vertraulichen Informationspool (INSI-Bereich).

Durch die Angabe von Kontaktdaten im Abschnitt 1.3 gestatte ich dem BSI die Kontaktaufnahme mit dem angegebenen Notfallkontakt sowie die elektronische Speicherung und Verarbeitung der hier angegebenen Daten entsprechend dem Abschnitt 1.3 „Datenschutz“ aus der Interessenbekundung zur Teilnahme an der Allianz für Cyber-Sicherheit.

Durch die Angabe von Kontaktdaten im Abschnitt 2 möchte ich die Institution ebenfalls für den UP KRITIS anmelden. Ich erkläre, dass alle angegebenen Personen sowie alle potenziellen Empfänger der angegebenen E-Mail-Adressen bzgl. der Einhaltung des TLP belehrt wurden und die Daten entsprechend dem 1.3 „Datenschutz“ aus der **Interessenbekundung** auch von UP KRITIS gespeichert und verarbeitet werden dürfen.

Änderungen bezüglich der angegebenen Daten werde ich unaufgefordert und unverzüglich mitteilen.

____.____.201__, _____ _____

Datum Ort Unterschrift Ansprechpartner