Antrag zur Aufnahme in das Sicherheitspaket des Hannover IT e.V.

Institution

Name	
Straße	
PLZ	Ort
Telefon (zentral)	E-Mail (zentral)
Anzahl Beschäftigte	Internetadresse
davon Berater	Social-Media

Geschäftsführung / Vertretungsbefugter

Vorname	Name
Akad. Grad	
Telefon (persönlich)	E-Mail (persönlich)

Ansprechpartner für die Initiative (falls abweichend)

Vorname	Name
Akad. Grad	
Telefon (persönlich)	E-Mail (persönlich)

Daten zum antragstellenden Unternehmen

Jeweils zum Stichtag der letzten zwei durchgeführten Rechnungsabschlüsse:	
Umsatz im Jahr 2016	Umsatz im Jahr 2017
Bilanzsumme im Jahr 2016	Bilanzsumme im Jahr 2017

Ich versichere mit meiner Unterschrift, dass die gemachten Angaben der Wahrheit entsprechen, unsere Mitarbeiter über die genannte Expertise verfügen und Unternehmen im Rahmen der Initiative nur nach bestem Wissen und Gewissen beraten werden. Mir ist bewusst, dass falsche Angaben zum Ausschluss meines Unternehmens von der Initiative oder zu rechtlichen Konsequenzen führen können.

Mir ist darüber hinaus bewusst, dass negative Rückmeldungen von Unternehmen von Hannover IT überprüft werden und bei einer Häufung von negativen Bewertungen mein Unternehmen ebenfalls von der Initiative ausgeschlossen werden kann.

Ort, Datum

Unterschrift, Stempel

Expertise zur Cybersicherheit

Hinweis:
- Bitte kreuzen Sie die Themen an, in denen Sie über Expertise verfügen und im Rahmen der Initiative gelistet werden möchten.
- Die Informationen werden genutzt, um die

Themenfelder gemäß der Website	Ja, wir möchten gelistet werden
Assurance, Audit und Zertifizierung Diese Domäne bezieht sich auf die Methoden, Frameworks und Tools, die die Grundlage für die Gewissheit schaffen, dass ein System oder Netzwerk funktioniert oder so konzipiert wurde, dass es am gewünschten Sicherheitsziel oder gemäß einer definierten Sicherheitsrichtlinie arbeitet.	☐
Datensicherheit und Datenschutz Diese Domäne umfasst Sicherheits- und Datenschutzfragen im Zusammenhang mit Daten, um (a) die Risiken für den Datenschutz und die Vertraulichkeit zu reduzieren, ohne die Zwecke der Datenverarbeitung zu beeinträchtigen, oder (b) den Missbrauch von Daten nach dem Zugriff durch autorisierte Stellen zu verhindern.	☐
Kryptologie Kryptologie fasst Kryptographie und Kryptoanalyse zusammen.	☐
Aus- und Weiterbildung Der Lernprozess des Erwerbs von Wissen, Know-how, Fähigkeiten und/oder Kompetenzen, die erforderlich sind, um Netzwerk- und Informationssysteme, deren Nutzer und betroffene Personen vor Cyberbedrohungen zu schützen.	☐
Operatives Incident Handling und digitale Forensik Diese Domäne bezieht sich auf die Theorien, Techniken, Werkzeuge und Prozesse zur Identifizierung, Sammlung, Erfassung und Bewahrung von digitalen Beweisen, die von Beweiskraft sein können.	☐
Menschliche Aspekte Diese Domäne umfasst das Zusammenspiel von Ethik, relevanten Gesetzen, Vorschriften, Richtlinien, Normen, Psychologie und dem Menschen innerhalb der Cybersicherheit.	☐
Identitäts- und Zugriffsmanagement (IAM) Diese Domäne deckt Sicherheitsbedenken im Zusammenhang mit der Authentifizierung, Zugriffskontrolle und Autorisierung von Personen und intelligenten Objekten beim Zugriff auf Ressourcen ab.	☐
Sicherheitsmanagement und Governance Dieser Bereich bezieht sich auf die Governance-Aktivitäten, Methoden, Prozesse und Instrumente, die auf das Management von Cyberrisiken abzielen.	☐
Netzwerke und verteilte Systeme Dieser Bereich umfasst die wissenschaftlichen und technologischen Kompetenzen im Zusammenhang mit dem Zusammenspiel von Cybersicherheitsnetzen und verteilten Systemen.	☐
Software- und Hardware-Sicherheitstechnik Dieser Bereich umfasst Sicherheitsaspekte im Lebenszyklus der Software- und Hardwareentwicklung und der Lieferkette wie Risiko- und Anforderungsanalyse, Architekturdesign, Code-Implementierung, Code-Überprüfung, Validierung, Verifizierung, Test, Bereitstellung, Laufzeitüberwachung des Betriebs und Zertifizierung.	☐

Sicherheitsmaßnahmen Maßnahmen und Indikatoren für die Informationssicherheit werden verwendet, um die Entscheidungsfindung zu erleichtern und die Leistung und Rechenschaftspflicht durch die Erhebung, Analyse und Berichterstattung relevanter leistungsbezogener Daten zu verbessern.	☐
Technologie und rechtliche Aspekte Diese Domain bezieht sich auf die rechtlichen und ethischen Aspekte im Zusammenhang mit dem Missbrauch von Technologie, der illegalen Verbreitung und/oder Vervielfältigung von Material, das unter die Rechte des geistigen Eigentums fällt, und der Durchsetzung der Gesetze im Zusammenhang mit Cyberkriminalität und digitalen Rechten.	☐
Theoretische Grundlagen der Sicherheitsanalyse und -gestaltung Diese Domäne bezieht sich auf die Verwendung von formalen Analyse- und Verifikationstechniken, um den theoretischen Nachweis von Sicherheitseigenschaften entweder im Software-, Hardware- und Algorithmen-Design zu erbringen.	☐
Vertrauensmanagement, -sicherung und -verantwortung Diese Domäne umfasst Vertrauensfragen im Zusammenhang mit digitalen und physischen Einheiten wie Anwendungen, Diensten, Komponenten oder Systemen. Trustmanagement-Ansätze können eingesetzt werden, um Sicherheits- und Rechenschaftsgarantien zu bieten.	☐

Nachweis über fachliche Expertise

Hinweis:

- Es sind mindestens 3 Referenzprojekte in den vergangenen 3 Jahren zu benennen.
- Referenzen können auch in Form von Präsentationen nachgewiesen werden.
- Für jedes Themenfeld, für das Sie gelistet werden möchten, muss mindestens eine Referenz nachgewiesen werden.

Welches Unternehmen wurde beraten? (Referenz 1, wird auf Wunsch vertraulich behandelt)

Name	
Straße	
Postleitzahl	Ort
Hauptgeschäftsfeld	
Geschäftsführung / Ansprechpartner	
Inhaltlicher Schwerpunkt der Beratung	
Für welches Themenfeld wird die Referenz eingebracht?	
Beratungszeitraum	Beratungsumfang

Welches Unternehmen wurde beraten? (Referenz 2, wird auf Wunsch vertraulich behandelt)

Name	
Straße	
Postleitzahl	Ort
Hauptgeschäftsfelder	
Geschäftsführung / Ansprechpartner	
Inhaltlicher Schwerpunkt der Beratung	
Für welches Themenfeld wird die Referenz eingebracht?	
Beratungszeitraum	Beratungsumfang

Welches Unternehmen wurde beraten? (Referenz 3, wird auf Wunsch vertraulich behandelt)

Name	
Straße	
Postleitzahl	Ort
Hauptgeschäftsfelder	
Geschäftsführung / Ansprechpartner	
Inhaltlicher Schwerpunkt der Beratung	
Für welches Themenfeld wird die Referenz eingebracht?	
Beratungszeitraum	Beratungsumfang

Kurzdarstellung der eigenen Organisation

Hinweis:

- Kurze Darstellung der Unternehmensentwicklung, der Kernkompetenzen und Hauptgeschäftsfelder
- Besondere Fähigkeiten, Beratungsleistungen, Expertisen
- Ideale Unternehmensgrößen, Tätigkeitsfelder & Branchen der durch Sie zu beratenden Unternehmen

(Stichpunkte, kann auch als Präsentation zur Verfügung gestellt werden)