Code of Conduct – Unser Verhaltenskodex (vers. 1.0)

Inhalt

Präambel

Das Cyber Security Cluster Bonn e.V. (CSCB) fördert und vernetzt Wissenschaft, Forschung & Lehre, Wirtschaft, Behörden und öffentliche Institutionen sowie sonstige Bereiche in der Region Bonn/Rhein-Sieg. Ziel ist es insbesondere dazu beizutragen eine Vernetzung von Kompetenzen im Cyberraum zu ermöglichen, die Cyber-Security Kompetenz im Land NRW nachhaltig zu stärken und die Region Bonn/Rhein-Sieg zu einem national und international beachteten und anerkannten Cyber-Security Standort zu entwickeln und auszubauen. Wir sind unabhängig und neutral und vernetzen unsere Mitglieder aktiv untereinander sowie mit führenden Technologie-, Geschäfts- und Servicepartnern. Über uns können Organisationen und Interessierte ihr Know-how mit dem Know-how anderer Mitglieder sowie mit exklusiven Serviceleistungen bündeln und ihr Leistungsprofil gezielt schärfen. So gestalten wir gemeinsam Cyber Security.

Anwendungsbereich

Dieser Code of Conduct findet Anwendung in allen öffentlichen und nicht-öffentlichen Äußerungen und Tätigkeiten der Mitglieder und Beiratsmitglieder bzw. entsprechender Mitarbeiter, wenn diese in einem unmittelbaren Zusammenhang mit dem CSCB oder einer Veranstaltung des CSCB stehen. Dies schließt insbesondere Zusammenhänge ein, in denen die Mitgliedschaft beim CSCB für Außenstehende in zeitlicher und räumlicher Nähe zu den Äußerungen und Tätigkeiten der oben genannten Personen erkennbar ist. Ebenfalls sind öffentliche Äußerungen in den (Sozialen) Medien sowie auf Webseiten und Blogs eingeschlossen, die explizit auf eine Mitgliedschaft hinweisen, z.B. durch die Verwendung des Logos oder des Namens des CSCB.

Ziele

Damit die Ziele der die Vereinsmitglieder des Cyber Security Clusters Bonn e.V. unterstützt werden können, sind eindeutige Verhaltensregeln unverzichtbar. Ziel des Code of Conduct ist es, das Verhalten zwischen Vereinsmitgliedern untereinander dergestalt zu regeln, dass diese in einem fairen und für beide Seiten förderlichen Miteinander tätig werden können.

1. Allgemeine Verhaltensregeln

1.1. Unsere Mitglieder kommunizieren stets offen, ehrlich, fair und respektvoll miteinander, da eine der jeweiligen Situation angepasste Kommunikation einer der wichtigsten Erfolgsfaktoren für eine erfolgreiche Zusammenarbeit darstellt.

1.2. Die Mitglieder des Cyber Security Cluster Bonn e.V. fördern Chancengleichheit und tolerieren keine Diskriminierung. Es gilt der Grundsatz, dass alle Menschen gleich zu behandeln sind, ungeachtet des Geschlechts, des Alters, der Hautfarbe, der ethnischen Herkunft, der sexuellen Identität und Orientierung, einer Behinderung, der Religionszugehörigkeit, Weltanschauung oder weiterer personenbezogener Merkmale.

2. Grundprinzipien der Cybersicherheit

Als Cyber Security Cluster Bonn e.V. ist uns ein idealer Umgang mit cybersicherheitsrelevanten Themen und Vorgängen wichtig. Wir befürworten, dass unsere Mitglieder sich an die nachfolgenden Punkte halten und diese fördern. Eine bewusste Nichtbeachtung der Punkte kann vom Verein als grober Verstoß gegen seine Werte und Vereinsinteressen gedeutet werden.

2.1. Die Mitgliedsunternehmen halten sich an Best Practice Maßnahmen im Bereich der Cyber Security und fördern die Entwicklung eigener Produkte auf der Grundlage von Security und Privacy by Design.

2.2. Die Mitgliedsunternehmen halten sich beim Umgang mit Sicherheitslücken in eigenen Produkten an die empfohlenen Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI). Der Verein fördert und unterstützt seine Mitglieder bei der Umsetzung einer Vulnerability Disclosure Policy.

2.3. Die Mitgliedsunternehmen halten Sicherheitslücken, über die sie Kenntnis besitzen, nicht bewusst zurück.

2.4. Die Mitgliedsunternehmen bekennen sich zum verantwortungsvollen Umgang mit Daten und melden Datenschutzverstöße anhand rechtlicher Vorgaben an die zuständigen Aufsichtsbehörden.

2.5. Die Mitgliedsunternehmen bieten keine Produkte an, die der branchenüblichen Definition von „Adware“ oder „Spyware“ oder Spam bzw. Schadsoftware entsprechen.

3. Zusammenarbeit von Mitgliedern

3.1. Der Cyber Security Cluster Bonn e.V. fördert die Zusammenarbeit seiner Mitgliedsunternehmen. So kann jedes Mitglied über das Cluster Management Unterstützung, Kompetenzen und Ressourcen anderer Mitgliedsunternehmen anfragen. Das Cluster Management vernetzt seine Mitglieder auf Basis der Verschwiegenheit und Vertraulichkeit sowie unter der Einhaltung datenschutzrechtlicher Grundprinzipien.

3.2. Der anfragende Partner verpflichtet sich kenntlich zu machen, ob seine Anfrage aufgrund eines nachweisbaren Kundenbedarfs oder ohne Kundenbedarf erfolgt und wird die involvierten Partner aktiv über den Fortgang seiner Anfrage informieren. Mitglieder haben Anfragen anderer Mitglieder zu beantworten und nehmen Aufträge nur an, wenn sie die notwendige Fachkompetenz haben und die erforderlichen zeitlichen und personellen Ressourcen vorhanden sind. Beim Zustandekommen einer neuen Zusammenarbeit sollten die Mitglieder eine angemessene schriftliche Vereinbarung abschließen, die die Aufgabenstellung, den zeitlichen Einsatz, den Einsatzort, die Vergütung bzw. die Ergebnisverwertung sowie die Art der Durchführung festlegt.

4. Keine aktive Abwerbung von Mitarbeitern und Kunden

4.1. Die im Cyber Security Cluster Bonn e.V. unmittelbar aktiven Mitglieder verpflichten sich wechselseitig, keine Arbeitnehmer von anderen Mitgliedern aktiv, d.h. durch gezielte Ansprache, für sich oder für Dritte abzuwerben. Damit ist nicht die eigenständige Bewerbung von Mitarbeitern gemeint.

4.2. Die im Cyber Security Cluster Bonn e.V. unmittelbar aktiven Mitglieder verpflichten sich wechselseitig, keine Kunden oder Geschäftspartner von anderen Mitgliedern aktiv, d.h. durch gezielte Ansprache oder durch die im Verein gewonnenen Kenntnisse und Informationen, für sich oder für Dritte abzuwerben. Damit sind nicht die eigenständigen Anfragen von Kunden gemeint.

5. Konflikte

5.1. Konflikte unter den Vereinsmitgliedern sollen, wenn möglich, erstmal untereinander besprochen und geklärt werden. Sollte dies nicht möglich sein, vermittelt das Clustermanagement aus unabhängiger Perspektive zwischen den Konfliktparteien und unterbreitet der Situation angemessenen Lösungsvorschläge. Wer der Überzeugung ist, dass ein Mitgliedsunternehmen oder eine in einem Mitgliedsunternehmen tätige Person mit seinem Verhalten gegen die Grundsätze und Regeln dieses Code of Conduct verstößt, der zeigt dies dem Cluster Management des Cyber Security Cluster Bonn e.V. schriftlich an. Sollte die Moderation über diesen Weg nicht möglich sein, wird auf Initiative des Cluster Managements eine unabhängige Mediationsstelle angerufen und die Durchführung einer Mediation, einer Schlichtung oder eines Schiedsverfahrens vorgeschlagen.

5.2. Ein Ausschluss aus dem Verein ist stets das letzte Mittel der Wahl. Bei schweren oder wiederholten Verstößen ist der Vorstand berechtigt, eine außerordentliche Kündigung der Vereinsmitgliedschaft zu erklären und hierüber – ohne Mitteilung der Gründe – die anderen Vereinsmitglieder durch die vereinsinternen Kommunikationskanäle zu informieren.