

Merkblatt zur IT Security Policy für externe Geschäftspartner der EnBW

1 Anwendungsbereich

Nach den Allgemeinen Einkaufsbedingungen des EnBW-Konzerns (Ziff. 2.5) sind Auftragnehmer der EnBW, die im Rahmen der Abwicklung eines Vertragsverhältnisses Zugang und Zugriff auf elektronische Informationen bzw. Informationssysteme der EnBW erhalten, verpflichtet, die Regelungen dieses Merkblattes strikt einzuhalten. Für alle Zweifelsfälle steht in Ergänzung dieses Merkblattes dem Auftragnehmer jederzeit die „IuK Security Policy externe Geschäftspartner“ der EnBW zur Einsicht und Beachtung offen.

Dieses Merkblatt richtet sich an alle Geschäftspartner, gleichviel ob ihnen ein IT-Arbeitsplatz-System der EnBW zur Verfügung gestellt wird oder sie mit eigenen Systemen oder mit Anschluss zu Ressourcen im EnBW-Kommunikationsnetzwerk auf die EnBW-Informationssysteme zugreifen.

2 Verantwortlichkeiten

Geschäftspartnern wird zum gegenseitigen Nutzen und zur Steigerung der Effizienz der Geschäftsabwicklung der Zugriff auf firmeneigene Informationen der EnBW gewährt und die Nutzung von EnBW-Systemen und –Netzen ermöglicht. Dies bedingt Sicherungsmaßnahmen zum Schutz der Vertraulichkeit, vor Computerviren, von Hackingangriffen und dergleichen. Dazu ist es zwingend erforderlich, die nachfolgenden Regeln und Grundsätze einzuhalten.

3 Vertraulichkeit

Jeder Geschäftspartner der EnBW ist verpflichtet, sämtliche Informationen, die er im Zusammenhang mit dem Zugriff auf die IT-Systeme der EnBW erhält oder ihm zugänglich sind streng vertraulich zu behandeln, sie insbesondere keinem Dritten zu offenbaren oder für andere als bestimmungsgemäße Zwecke zu verwenden. Der Geschäftspartner hat bei Beendigung der Beauftragung erhaltene Unterlagen unaufgefordert zu vernichten oder auf Verlangen zurückzugeben. Die Verpflichtung zur Vertraulichkeit besteht über die jeweilige Zusammenarbeit hinaus auf Dauer fort.

4 Generelle Regelungen des Datenzugangs/ -zugriffs

Jeder Geschäftspartner hat bei Zugang/ Zugriff auf die IT-Systeme der EnBW folgende Grundsätze zu beachten:

- › Der Zugriff darf nur über die jeweils zur Verfügung gestellten Endgeräte und für die vereinbarten Zwecke und Aufgaben erfolgen.
- › Die hinterlegten Schutzmechanismen (Kennungen und Passwörter) müssen personenscharf verwandt werden. Eine Weitergabe oder Offenlegung für Dritte ist in jedem Fall zu vermeiden.
- › Besondere Sicherungseinstellungen, -systeme oder sonstige Vorkehrungen (z.B. zum Schutz vor Computerviren) dürfen nicht außer Betrieb genommen, umgangen oder in sonstiger Weise verändert werden.
- › Die Zuschaltung/ Anbindung eigener Systeme des Geschäftspartners an das Kommunikationsnetzwerk der EnBW ist strikt zu vermeiden.
- › Die Mitnahmen von Dokumenten, Arbeitsergebnissen oder IT-Systemen außerhalb der Geschäftsräume der EnBW ist grundsätzlich nicht erlaubt und bedarf der vorherigen schriftlichen Genehmigung der EnBW und in Einzelfällen wie Betriebs- und Geschäftsgeheimnissen der Abstimmung mit dem jeweiligen Security-Manager.
- › Die Nutzung der E-Mail Konfiguration der EnBW bedarf der vorherigen Einweisung und Nutzung unter Einhaltung der internen Regelungen der EnBW („E-Mail-Knigge“). Insbesondere ist die automatisierte Weiterleitung empfangener E-Mails an externe Postfächer untersagt.
- › Der Geschäftspartner hat zudem sämtliche einschlägigen normativen Bestimmungen insbesondere datenschutzrechtlicher Art strikt zu beachten.

5 Besondere Regelungen der Datennutzung im Einzelfall

- › Die EnBW behält sich vor, bei Umgang des Geschäftspartners mit besonders sensiblen oder geheimhaltungsbedürftigen Daten der EnBW im Einzelfall zuvor ein besonderes Sicherheitsniveau festzulegen und besondere Schutzanordnungen zu treffen.
- › Bei Verdacht auf nicht automatisch erkennbare oder zu beseitigende Computerviren oder Ablaufproblemen der Virenschutzprogramme ist unverzüglich die zuständige Stelle der EnBW zu benachrichtigen.
- › Sofern der Geschäftspartner Schwachstellen und Vorfälle mit möglichen Auswirkungen auf die Informationssicherheit erkennt, meldet er diese umgehend der verantwortlichen Stelle der EnBW.

- › Die Einhaltung der Maßnahmen zur IT-Security wird durch EnBW kontrolliert und insbesondere durch den Datenschutzbeauftragten und /oder den Konzernbevollmächtigten IuK-Security der EnBW überwacht.

- › Ein Verstoß gegen die Bestimmungen des Merkblattes kann – unbeschadet der sonstigen Rechte aus dem Vertragsverhältnis mit dem Geschäftspartner – zum sofortigen Entzug der Zugangs-/ Zugriffsberechtigungen auf die IT-Systeme der EnBW führen.