Informationssicherheitsbestimmungen

für die
„Netzdienstleistung eHealth Interexchange (HEALIX)
zum sicheren Transport von Daten aus dem Gesundheits- und Sozialwesen in einem geschlossenen Netzwerk“

„HEALIX Informationssicherheitsbestimmungen“

Alle personenbezogenen Bezeichnungen des Textes sind jeweils geschlechtsneutral formuliert zu verstehen.

Präambel

Das vorliegende Dokument legt die Vorgaben zur Gewährleistung eines angemessenen Sicherheitsniveaus für den Betrieb von Informations- und Kommunikationstechnologie (IKT) Services bei der Nutzung der Netzdienstleistung HEALIX gesamtheitlich fest.

Die letztgültige Fassung ist unter www.healix.at abrufbar.

Informationssicherheit ist ein Thema, das alle Nutzer des Kommunikationsdienstes HEALIX betrifft. Engagiertes, kooperatives und verantwortungsbewusstes Handeln ist daher insbesondere bei der Gewährleistung der Sicherheit notwendig.

Da es sich um ein langfristig orientiertes Grundlagendokument handelt, sind hier technische und organisatorische Einzelheiten zu Sicherheitsmaßnahmen und deren Umsetzung bei den Nutzern des Kommunikationsdienstes HEALIX nicht Bestandteil, es wird aber vorausgesetzt, dass eine eigenverantwortliche Realisierung durch die HEALIX Teilnehmer und die HEALIX Kooperationspartner erfolgt.

Eine der Intentionen in der Netzdienstleistung HEALIX ist ein funktionierendes Vorfallsmeldesystem zwischen den HEALIX Teilnehmern und/oder den HEALIX Kooperationspartnern. Damit wird die Grundlage für die Verbesserung, die Kontinuität und Stabilität der IKT Services der HEALIX Teilnehmer geschaffen.

§ 1 Definitionen

(1) Vorfall:
Eine Störung (Incident) ist ein Ereignis, das nicht Teil des Standardbetriebs des IKT Services ist und eine Unterbrechung oder Minderung der Qualität des IKT Service bei einem oder mehreren HEALIX Teilnehmern verursacht und/oder die Funktionalität des elektronischen Verkehrs mit Gesundheitsdaten im Kommunikationsdienst HEALIX negativ beeinflusst.
(2) Vorfallsmeldung:
Ist eine Information an die anderen HEALIX Teilnehmer und/oder HEALIX Kooperationspartner über die Wahrnehmung eines Vorfalls.

§ 2 Allgemeine Sicherheitsbestimmungen der Netzdienstleistung HEALIX

(1) Die Nutzer der Netzdienstleistung HEALIX verpflichten sich gegenseitig im Interesse der Informationssicherheit, die Wahrnehmung eines Vorfalls und die Reaktion auf einen Vorfall, der sich auf die Funktionalität des elektronischen

Verkehrs mit Gesundheitsdaten negativ auswirkt, den anderen HEALIX Teilnehmern oder HEALIX Kooperationspartnern ohne unnötigen Aufschub mitzuteilen.

(2) Die Nutzer verpflichten sich gegenseitig im Interesse der Informationssicherheit eine Reaktion auf die Wahrnehmung eines Vorfalls bzw. eine Reaktion auf eine Vorfallsmeldung zu setzen. Die Reaktion auf einen Vorfall bzw. der Vorfallsmeldung hat zum Ziel, dass die nachhaltigen Auswirkungen von Fehlern auf Geschäftsprozesse der Nutzer des Kommunikationsdienstes HEALIX (insbesondere der HEALIX Teilnehmer) minimiert bzw. verhindert werden. Zusätzlich soll die Reaktion auf einen Vorfall bzw. der Vorfallsmeldung proaktiv das Auftreten von Störungen, Problemen und Vorfällen vermeiden.

(3) Die von den Nutzern zu treffenden Maßnahmen gemäß diesen Bestimmungen erfolgen auf eigene Kosten und nach dem jeweiligen Stand der Technik.

(4) Die Nutzer haben in ihrem eigenen Wirkungsbereich Maßnahmen zum Schutz der Vertraulichkeit der Vorfallsmeldung laut § 1 Abs. (2) auf technischer, organisatorischer und personeller Ebene (in weiterer Folge „auf mehreren Ebenen“ bezeichnet) zu treffen.

(5) Die Nutzer haben beim Aufbau eines Computer Emergency Response Team des Kommunikationsdienste HEALIX mitzuwirken.

§ 3 Sicherheitsbestimmungen HEALIX Teilnehmer

(1) Der HEALIX Teilnehmer hat in seinem Zuständigkeitsbereich insbesondere Regeln für den Betrieb der Netzdienstleistung HEALIX sowie einen Aktionsplan mit Informationspflicht bei Störfällen festzulegen und die darin definierten Ansprechstellen den anderen HEALIX Teilnehmern über den zugangsbeschränkten HEALIX Teilnehmerbereich von www.healix.at zur Kenntnis zu bringen.

(2) Der HEALIX Teilnehmer hat mindestens einmal jährlich eine Sicherheitsrevision durchzuführen oder zu veranlassen. Die Sicherheitsrevision muss sich auf das erlassene Regelwerk des HEALIX Teilnehmers beziehen, die den in der HEALIX Informationssicherheitsbestimmungen beschriebenen Maßnahmen entsprechen. Die Metainformationen (insbesondere Organisationsbezeichnung, Revisionsdatum, Revisionsverantwortlicher, Revisionsstatus sowie Organisationsansprechpartner) des Sicherheitsrevisionsberichtes sind den anderen HEALIX Teilnehmern über den zugangsbeschränkten HEALIX Teilnehmerbereich von www.healix.at zur Kenntnis zu bringen.

(3) Der HEALIX Teilnehmer hat an der Nahtstelle zur Netzdienstleistung HEALIX eine Firewall zu betreiben oder betreiben zu lassen.

(4) Der HEALIX Teilnehmer hat in seinem eigenen Wirkungsbereich oder in dem an ihn übertragenen Wirkungsbereich Maßnahmen zum Schutz auf mehreren Ebenen zu setzen oder setzen zu lassen (insbesondere: aktueller Virenschutz in Letztversion, Verwendung aktueller Versionen aller eingesetzten Betriebssysteme und Software, …).

(5) Der HEALIX Teilnehmer hat für seinen eigenen Wirkungsbereich in einem Zyklus von mindestens 24 Monaten Ausbildungsmaßnahmen zur Verbesserung des Sicherheitsbewusstseins im Ausmaß von mindestens 4 Stunden (entsprechen 180 Unterrichtsminuten) pro betroffenen Personenkreis zu treffen.

§ 4 Sicherheitsbestimmungen HEALIX Kooperationspartner

(1) Der HEALIX Kooperationspartner hat in seinem Wirkungsbereich das - Sicherheitsbewusstseins für die Interessen der Netzdienstleistung HEALIX zu unterstützen und zu fördern.

§ 5 Maßnahmenkatalog der Netzdienstleistung HEALIX

(1) Durch einen Vorfall, der in seiner Auswirkung die Netzdienstleistung HEALIX massiv beeinträchtigt, wird eine vorübergehende Netztrennung zwischen dem HEALIX Teilnehmer und dem betreffenden Gesundheitsknoten durchgeführt.
(2) Durch einen Vorfall, der in seiner Auswirkung die Netzdienstleistung HEALIX beeinträchtigt, wird der HEALIX Teilnehmer in einer nichtöffentlichen Benachrichtigung aufgefordert, innerhalb einer festgesetzten Frist die Bereinigung vorzunehmen.
(3) Durch einen Vorfall, der in seiner Auswirkung die Netzdienstleistung HEALIX wiederholt beeinträchtigt, wird der HEALIX Teilnehmer in einer öffentlichen Benachrichtigung der Netzdienstleistung HEALIX aufgefordert, innerhalb einer festgesetzten Frist die Bereinigung vorzunehmen.
(4) Der HEALIX Teilnehmer wird über seine Ansprechpartner, die in seinen Aktionsplan bekanntgegeben sind, über eine Maßnahme in Kenntnis gesetzt und die weitere Vorgangsweise mit dem HEALIX Teilnehmer abgestimmt.