jobcenter StädteRegion Aachen

Verfügung 10/2014

Aktenzeichen: II-5214
Verfasser: Herr Kreitz

IT-Sicherheit

I. Einleitung

Der Themenkomplex IT-Sicherheit beinhaltet alle technischen Maßnahmen zur Verringerung des Gefährdungspotenzials für IT-Anwendungen und -Systeme. Alle mit dem Gefährdungspotenzial in Zusammenhang stehenden Schutzmaßnahmen, wie die Entwicklung von Sicherheitskonzepten, die Vergabe von Zugriffsberechtigungen und die Implementierung von Sicherheitsstandards, sind Aspekte der IT-Sicherheit. IT-Sicherheit ist die technische Umsetzung der Sicherheitskonzepte unter wirtschaftlichen Aspekten.

Die IT-Sicherheit umfasst alle gefährdeten und daher schützenswerten Einrichtungen, Systeme und Personen. Dazu gehören u.a. Gebäude, Netze, Hardware und Software sowie die an den Systemen Arbeitenden. Ziel der IT-Sicherheit ist es, die Verfügbarkeit von Systemen und Daten sicherzustellen, die Vertraulichkeit zu gewährleisten, damit weder Unbefugte auf Dateien zugreifen können und die Dateien auch bei der Übertragung weiterhin vertraulich bleiben, die Sicherstellung der Authentizität und der Integrität http://www.itwissen.info/definition/lexikon/Integritaet-integrity.html der Daten.

II. Eigene Entscheidung und Absicht

Ereignisse aus der Vergangenheit zeigen, die Sicherheit der IT betrifft uns alle, sowohl als Bürger/In in einer Informationsgesellschaft als auch als Mitarbeiter/In des Jobcenters im Umgang mit der IT.
Sozialdaten, die im Internet öffentlich zugänglich sind, personenbezogene Daten, mit denen gehandelt wird und immer wieder auftretenden Virenmeldungen sind nur die Spitze des Eisbergs.
Kaum berichtet wird von den vielen „kleinen“ IT-Sicherheitsvorfällen.
Organisationen, die in IT-Sicherheitsvorfälle verwickelt sind, können einen immensen Vertrauensverlust erleiden, sind ggf. Haftungsansprüchen ausgesetzt und müssen unter Umständen einen nachhaltigen Imageschaden hinnehmen.
Ziel dieser Verfügung ist es, die Mitarbeiter des Jobcenters StädteRegion Aachen verstärkt für das Thema der IT-Sicherheit zu sensibilisieren.

III. Informationsquellen, Ansprechpartner und E-Mail-Postfach

III.1. Informationsquellen

Es gibt eine Vielzahl von Informationsmöglichkeiten zum Thema IT-Sicherheit.
Damit diese Vielzahl nicht verwirrend wirkt, führen wir hier einige wesentlichen Infoquellen auf.

Intranet des Jobcenter StädteRegion Aachen:
http://intranet.jobcenter-staedteregion-aachen.de/service-fuer-mitarbeiter/sonderstellen/datenschutzbeauftragter/it-sicherheit.html

Zentrale Ablage des Jobcenter StädteRegion Aachen:
\\Dst.baintern.de\dfs\311\Ablagen\D31192-JC-StaedteRegion-Aachen-zentral\Verwaltung\05_zentrale_Dienste\Datenschutz\5214_Sicherheit_und_Datenschutz\IT_Sicherheit

III.2. Ansprechpartner

Ansprechpartner sind die IT-Sicherheitsbeauftragten des Jobcenter StädteRegion Aachen.

Erforderlich ist ein IT-Sicherheitsbeauftragter pro Geschäftsstelle.
Eine Übersicht der IT Sicherheitsbeauftragten finden Sie im Intranet an dieser Stelle.

III.3. E-Mail-Postfach

Fragen und Meldungen sind an folgendes Organisationspostfach zu richten:

_BA-Jobcenter Aachen-IT-Sicherheit (intern)
Jobcenter-Aachen.IT-Sicherheit@jobcenter-ge.de (extern)

IV. Qualifizierung der Mitarbeiter

IV.1. Grundlage Modul „IT-Sicherheit“ (Web-Based-Training) IT-Sicherheit

Gemäß der „HEGA 12/2008 -32_ Umsetzung der ganzheitlichen IT-Sicherheitsorganisation und Qualifizierung zur IT-Sicherheit in der BA“ ist jeder Beschäftigte verpflichtet, das Selbstlernmodul durchzuarbeiten.

IV.2. neue Mitarbeiter

Für neu eingestellte Mitarbeiter/innen ist die Durcharbeitung des WBT verpflichtend vorgegeben. Als maximale Zeitspanne gelten zwei Monate nach Einstellungsdatum.

Die Einhaltung wird über die Checkliste Neueinstellung überwacht.

IV.3. Stammkräfte

Aufgrund dessen das die Durcharbeitung des WBT bei den meisten Mitarbeiterinnen und Mitarbeitern einige Zeit zurück liegt, ist eine einmalig aktuelle Durcharbeitung verpflichtend. Dies ist durch jeden Mitarbeiter/ jede Mitarbeiterin bis zum 31.08.2014 zu erledigen.

Im Monat Oktober 2014 sind die bei Team 512 eingegangenen Durcharbeitungsbestätigungen (siehe: IV.5. Dokumentation) mit einer aktuellen Mitarbeiterliste abzugleichen.

Mitarbeiter deren Bestätigung fehlt, sind mit einer E-Mail incl. Erledigungsfrist von 4 Wochen an die Durcharbeitung und die Zusendung der Bestätigung zu erinnern.
Die jeweilige Führungskraft ist über diese Mail (per: Cc) in Kenntnis zu setzen.

IV.4. Fundstelle und Struktur des WBT

Fundstelle:
Das WBT finden Sie in der BA-Lernwelt unter:
IT-Verfahren / Informationsverarbeitung --- IT-Sicherheit---Selbstlernangebote

Struktur des WBT:
Das WBT hat folgende Kapitel (in Klammern die voraussichtliche Bearbeitungszeit):

1. Warum geht IT-Sicherheit alle an? (3 min)
2. Klassifizierung von Geschäftsinformationen (12 min)
3. Sicherer Umgang mit Geschäftsinformationen (15 min)
4. Zugangs- und Zugriffsschutz (18 min)
5. Nutzung von E-Mail (17 min)
6. Nutzung des Internets (10 min)
7. Nutzung des Intranets (3 min)
8. Schutz vor Schadensprogrammen (5 min)
9. Installation und Nutzung von IT-Komponenten (5 min)
10. Mobiles Arbeiten (7 min)

In Summe ergibt sich eine Bearbeitungszeit von ca. 1 ½ Stunden. Das WBT kann kapitelweise abgearbeitet werden und enthält in jedem Kapitel einen kleinen Frageteil als Lernhilfe (Wissenstest). Die Forderung nach Barrierefreiheit ist im WBT erfüllt.

IV.5. Dokumentation

Am Ende des Selbstlernprogramms ist der Ausdruck einer Bestätigung über die Bearbeitung vorgesehen.
Die jeweilige Führungskraft überwacht die Abarbeitung des WBT.
Die Ausdrucke sind über die Führungskraft an Team 512 zu senden.

VI. Implementierung von sensiblen Themen der IT-Sicherheit in den Teambesprechungen

Halbjährlich sind die Mitarbeiter zu einem gewissen Punkt bzw. Punkte der IT-Sicherheit besonders durch die Führungskräfte zu sensibilisieren.

Die Durchführung ist schriftlich zu dokumentieren.

Die Themen der Sensibilisierung werden durch die IT-Sicherheitsbeauftragten mitgeteilt.

VII. Risikoanalyse und Durchführung

.

Diesbezüglich wird auf das Konzept zum Berichtswesen der IT-Sicherheit als Bestandteil des Internen Kontrollsystems (IKS) verwiesen.

Link zum Konzept

VIII. Berichtswesen

Der Federführende erstellt jährlich einen Bericht über den Sachstand der IT-Sicherheit incl. Umsetzungsstand der Punkte IV. bis VII.

Der Bericht wird jährlich zum 31.10. der Geschäftsführung vorgelegt.

Eschweiler, 09.05.2014

Stefan Graaf
Geschäftsführer