Raiffeisen Informatik Center Steiermark

R R
Z _

safe data,
great business.

Information Security Policy für Geschäftspartner

Raiffeisen Informatik Center Steiermark
Raiffeisen Rechenzentrum

Dokument Eigentümer	Hefler
Version	1.3
Versionsdatum	22.08.2013
Status	Freigegeben
Vertraulichkeitsklassifizierung	Öffentlich

Inhaltsverzeichnis

1 Gültigkeit

Die Geschäftspartner der Raiffeisen Rechenzentrum GmbH, in weiterer Folge RRZ genannt, und der Raiffeisen Informatik Center Steiermark GmbH, in weiterer Folge RICS genannt, verpflichten sich dazu, die in diesem Dokument festgelegten Vorgaben einzuhalten. Verstöße gegen diese Vorschriften sind den angeführten Unternehmen umgehend zu melden. Als Geschäftspartner werden Kunden und Lieferanten des RICS und des RRZ festgelegt.

Dieses Dokument muss den Geschäftspartnern zur Verfügung gestellt werden, um diese in der Einhaltung der Vorgaben zu unterstützen.

Die in diesem Dokument festgehaltenen Vorgaben richten sich an alle Geschäftspartner denen ein Zugang zu elektronischen Daten, Informationen und Ressourcen vor Ort mit RRZ bzw. RICS eigener Hardware oder über entfernte Arbeitsplätze mit RRZ bzw. RICS fremder Hardware ermöglicht wird.

1.1 Verantwortung

Das RRZ bzw. RICS gewährt den Zugriff auf unternehmensbezogene Daten, Informationen und Ressourcen zum gegenseitigen Nutzen und zur Verbesserung der Effizienz der Geschäftsprozesse. Dies erfordert Maßnahmen zur Gefahrenabwehr gegen Angriffe auf Computersysteme sowie zum Schutz der Vertraulichkeit, Verfügbarkeit und Integrität der Daten und Informationen. Zu diesem Zweck ist es unbedingt notwendig, dass die Geschäftspartner des RRZ bzw. RICS nachfolgende Regeln und Prinzipien einhalten.

2 Vertraulichkeit

Jeder Geschäftspartner des RRZ bzw. RICS verpflichtet sich, sämtliche RRZ bzw. RICS bezogenen Daten und Informationen streng vertraulich zu behandeln. Insbesondere ist des den Geschäftspartnern streng untersagt RRZ bzw. RICS bezogene Daten an Dritte weiterzugeben. Weiters dürfen diese Daten und Informationen nur für genau jenen Verwendungszweck herangezogen werden, für den sie bestimmt sind. Jeglicher Missbrauch ist untersagt.

Nach Beendigung der Geschäftspartnerschaft (Auslauf der vertraglichen Vereinbarung, vorzeitige oder reguläre Kündigung) verpflichtet sich der Geschäftspartner dazu sämtliche ihm vorliegende RRZ bzw. RICS bezogenen Daten und Informationen entweder unaufgefordert unwiederbringlich zu zerstören, oder auf Anforderung des RRZ bzw. RICS diese wieder zu retournieren.

Die Verpflichtung zur Einhaltung der Vertraulichkeit in Bezug auf die unternehmensbezogenen Daten des RRZ bzw. RICS gilt dauerhaft und bleibt über die Dauer der jeweiligen Zusammenarbeit bestehen.

3 Allgemeine Bestimmungen für den Datenzugriff

Folgende Vorgaben sind von den Geschäftspartnern einzuhalten:

- Der Zugriff auf Daten, Informationen und Ressourcen ist ausschließlich unter Verwendung zuvor vereinbarter Methoden und technischer Komponenten zulässig.
- Daten, Informationen und Ressourcen sind ausschließlich für die vereinbarten Zwecke und Aufgaben zu nutzen.
- Zugangsdaten wie Benutzernamen und Passwörter müssen jeweils einem einzigen Benutzer zugeordnet werden. Eine Veröffentlichung oder Weitergabe an Dritte ist untersagt.
- Es müssen entsprechende Sicherheitsvorkehrungen zum Schutz vor technischen (z. B. Computerviren, Hacker, Exploits) und nicht-technischen (z. B. Social Engineering) Angriffen umgesetzt sein.
- Die Einbindung von IT Systemen des Geschäftspartners in das Kommunikationsnetz des RRZ bzw. RICS ist untersagt
- Die Weitergabe von Daten, Informationen, Dokumenten oder IT-Systemen ohne vorherige schriftliche Zustimmung des RRZ bzw. RICS ist untersagt
- Daten und Informationen mit Bezug auf das RRZ bzw. RICS enthalten, dürfen nicht ohne ausdrücklich Zustimmung des RRZ bzw. RICS an Dritte weitergeleitet werden.
- Der Geschäftspartner verpflichtet sich zur Einhaltung aller relevanten Vorschriften und gesetzlichen Vorgaben. Insbesondere zur Einhaltung der Bestimmungen des Datenschutzgesetzes.

4 Spezielle Regelungen

- Das RRZ bzw. RICS behält sich das Recht vor, das vom Geschäftspartner geforderte Sicherheitsniveau im Anlassfall zu erhöhen.
- Erkannte Schwachstellen in der IT-Security oder der Eintritt von Sicherheitsvorfällen auf Seiten des Geschäftspartners, welche potentielle Auswirkungen auf das RRZ bzw. RICS haben, müssen dem RRZ bzw. RICS umgehend berichtet werden.
- Bei Verdacht auf nicht automatisch erkennbare oder zu beseitigende Computerviren oder Ablaufproblemen der Virenschutzprogramme ist das RRZ bzw. RICS umgehend von diesem Umstand in Kenntnis zu setzen.
- Die Einhaltung der Maßnahmen zur Sicherstellung der Informationssicherheit wird vom RRZ bzw. RICS überwacht.
- Ein Verstoß gegen die in diesem Dokument beschriebenen Vorgaben kann zum sofortigen Entzug der Zugangs- oder Zugriffberechtigungen auf die IT-Systeme des RRZ bzw. RICS führen.
- Das RICS bzw. RRZ behält sich das Recht vor, die Einhaltung der in diesem Dokument festgelegten Regelungen vor Ort zu prüfen.

5 Zugriffsschutz

5.1 Umgang mit Passwörtern

Automatisierte Systeme müssen individuelle zugewiesene Konten verwenden, die eine regelmäßige Passwortänderung erfordern. IT-Sicherheitsrichtlinien, Vorgehensweisen und Standards müssen implementiert werden, und die Mitarbeiter müssen entsprechend geschult werden.

5.2 Schutz vor Missbrauch

Es muss ein System vorhanden sein, das den Missbrauch von IT-Ressourcen, einschließlich des unbefugten Zugriffs und der Verfälschung oder Änderung von Geschäftsdaten identifiziert. Alle gegen das System verstoßenden Personen müssen dafür disziplinarrechtlich zur Rechenschaft gezogen werden.

6 Bewusstseinsbildung

Geschäftspartner des RRZ bzw. RICS sind dazu angehalten innerbetriebliche bewusstseinsbildende Maßnahmen im Bereich der Informationssicherheit zu institutionalisieren. Ziel ist es dass Mitarbeiter Bedrohung erkennen und die zuständigen Stellen melden. . Vor allem Schulungen in der Erkennung und Abwehr von sog. Social Engineering Attacken sollten flächendeckend und regelmäßig abgehalten werden.

Dokumentenkontrolle

Dokumentenkontrolle	
Titel	Information Security Policy für Geschäftspartner
Version	1.3
Status (Entwurf / Freigegeben)	Freigegeben
Ersetzt Version	1.3
Eigentümer	Hefler
Revisionsdatum	22.08.2013
Datum der nächsten Revision	
Dateiname	ISP_externe_Partner_V1.3.docx
Anzahl Seiten	6
Druckdatum	Zuletzt gedruckt 04.09.2013 13:12:00

Dokumenten Historie

Revisions-datum	Version Nr.	Änderungen	Autor	Editor	Begutachter	Genehmiger
07.10.2010	1.0	Erstellung	Markus Hefler	Markus Hefler	Dietmar Schlar	Dietmar Schlar
20.07.2011	1.1	Anpassungen Kapitel 3 und Kapitel 6.	Markus Hefler	Markus Hefler	Daniela Berger	Dietmar Schlar
27.09.2011	1.2	Ergänzung der Möglichkeit, Audits vor Ort durchzuführen	Markus Hefler	Markus Hefler	Daniela Berger	Dietmar Schlar
22.08.2013	1.3	Anpassung neues Format und Wording RRZ	Markus Hefler	Daniela Berger	Markus Hefler	Dietmar Schlar