Anhang B: Katalog Technische und organisatorische Maßnahmen

Dieses Dokument gilt als Ergänzung zu den im Verfahrensverzeichnis angeführten Punkt 5. Technischorganisatorische Maßnahmen (TOMs).

5.1. Vertraulichkeit

Nur berechtigte Personen erhalten Zugriff auf Informationen. Sämtliche Mitarbeiter wurden über die Datenschutzbestimmungen informiert und erhalten laufend Schulungen. Die Maßnahmen sind im Dienstvertrag und in der Verpflichtungserklärung festgehalten. Es gelten die internen Benutzerrichtlinien unserer Unternehmensgruppe u.a. zum Thema Passwortrichtlinien und Berechtigungs- sowie Freigabeverwaltungen. Für die User gilt die Anweisung nicht auf ihre lokalen Geräte, sondern auf zentrale Sicherheitslaufwerke zu speichern. Die Ordner und sensible Informationen werden versperrt aufbewahrt. Weiters werden vertrauliche Dokumente am allgemeinen Drucker nur nach Codeeingabe im Gerät ausgedruckt.

5.2 Integrität

Die unberechtigte Manipulation der Daten bzw. die ungewollte Veränderung von Daten wird verhindert. Im Auftragsformular wird der Kunde über die Art und Notwendigkeit seiner Daten und deren Verarbeitung informiert. Intern sind PC, Notebook und Smartphone passwortgeschützt. Die Zugriffe werden protokolliert und es werden VPNs genutzt. Zur technischen Sicherheit sind Firewalls und ein Virenschutz im Einsatz. Im Asset Management sind alle Gerätschaften verzeichnet. Hier wird der Verlauf bei Ein- und Austritten, sowie die Vernichtung der Geräte dokumentiert. Weiters werden alle Schlüssel und Zutrittskarten zentral verwaltet, unter hohen Sicherheitsstandards verwahrt und deren Ausgabe protokolliert.

5.3 Verfügbarkeit

Die Verarbeitung von Daten muss immer einem Zweck dienen. Die Erfüllbarkeit dieses Zweckes muss bestmöglich gesichert werden. Kritische Hardware wird serviceciert und regelmäßig getauscht. Weiters verfügen wir über ein Ersatzteillager, um die höchstmögliche Verfügbarkeit zu garantieren. Die laufende Datensicherung erfolgt an einem anderen Standort. Weiters ist die operative Umgebung komplett von der Entwicklungsumgebung getrennt. Jegliche Software (Datenverarbeitung, Betriebssystem ...) wird laufend aktualisiert und entspricht den neuesten Sicherheitsstandards.

5.4. Andere Maßnahmen

Die Brennercom Tirol GmbH ist seit dem 08.03.2007 nach der internationalen Norm ISO 27001 für Informationssicherheit zertifiziert. Wir arbeiten an der fortlaufenden Verbesserung der Sicherheitsmechanismen in unseren Abläufen und Systemen zum Schutz sämtlicher Daten und Werte. Weiters werden die Anforderungen und Vorschriften gemäß Telekommunikationsgesetz 2003 eingehalten.

5.4.1 Physische Maßnahmen

Für den Schutz der Räumlichkeiten gelten am Hauptsitz in der Eduard-Bodem-Gasse 8 in Innsbruck die gleichen Regelungen wie in den Kollokationslokalitäten und dem Backup Standort unseres Datacenters. Der Zutritt zu den Räumlichkeiten ist videoüberwacht und alarmgesichert. Jeder Zugang wird protokolliert. Die Rechenzentren im 1.OG sind gesondert videoüberwacht und nur für autorisierte Personen innerhalb der Unternehmensgruppe zugänglich. Zusätzlich werden die Gebäude durch einen Wachdienst gesichert. Im Rechenzentrum ist eine Überwachung der Temperatur, Feuchtigkeit sowie eine automatische Löschanlage mit Novac 1230 vorhanden. Bei Abweichungen von den Standardwerten wird sofort eine Meldung verschickt. Sämtliche Schränke sind alarmgesichert und bei jeder Öffnung wird ein automatisiertes Mail verschickt. Im Falle eines Stromausfalles gibt es Batterie Anlagen und ein Diesel Notstromaggregat um die unterbrechungsfreie Stromversorgung zu gewährleisten. Sämtliche Anbindungen (Strom, Klima, Netzwerk …) sind redundant. Es bestehen jeweils getrennte Netzwerke und Anbindungen für die beiden Rechenzentren sowie für das interne Netz. Für den Eingangs- und Sitzungsbereich wurde ein eigenes Gäste WLAN eingerichtet. Externe Personen haben während und außerhalb der Geschäftszeiten ausschließlich unter Aufsicht eines zuständigen Mitarbeiters Zutritt zu den Räumlichkeiten.

5.4.2 Partnerschaften

Für sämtliche Dritte wie Lieferanten, Partner und Sub-Auftragsdatenverarbeiter sehen die vertraglichen Übereinkünfte, wie zum Beispiel der Vertrag für Informationssicherheit mit Partner, Rahmenvertrag oder Lizenznutzungsvereinbarung, eine mindestens äquivalente Umsetzung der Datenschutzrichtlinien gegenüber unserer Bestimmungen vor. Der Datenaustausch erfolgt teils über gesicherte Online Portale. Sämtliche Zugriffe werden protokolliert.