1. VERWENDEN SIE MÖGLICHST EINEN BROWSER MIT 128 BIT SSL-VERSCHLÜSSELUNG

Die aktuellen Versionen der gängigen Browser (Microsoft Internet Explorer, Apple Safari, Mozilla Firefox oder Opera) sind auf diesen Standard ausgelegt.

2. SCHÜTZEN SIE IHREN PC MIT AKTUELLEN VIRENSCHUTZPROGRAMMEN UND EINER FIREWALL
Installieren Sie eine Virenschutzsoftware auf Ihrem PC und aktualisieren Sie diese regelmäßig. Stellen Sie sicher, dass Ihr Rechner frei von Viren, Würmern und Trojanern/Backdoors ist. Wir empfehlen Ihnen, Ihren Rechner mit einer Firewall und einer Anti-Spy-Software auszustatten und diese regelmäßig zu aktualisieren.

Bitte nehmen Sie zur Kenntnis, dass wir Ihnen lediglich einen Internetzugang zur Verfügung stellen, der über keinerlei Virenschutz und keine Firewall verfügt.

3. HALTEN SIE IHR BETRIEBSSYSTEM AUF DEM AKTUELLEN STAND
Installieren Sie die entsprechenden Updates und Patches für das Betriebssystem Ihres PC zeitnah und regelmäßig.

4. SCHÜTZEN SIE IHRE DATEN AUCH FÜR DEN FALL DES VERLUSTES IHRES RECHNERS
Ihren PC und die darauf gespeicherten wichtigen Dateien sollten Sie mit Passwörtern sichern. Diese sollten regelmäßig geändert werden. Speichern Sie die Passwörter nicht auf Ihrer Festplatte ab. Stellen Sie Ihren Rechner auch nur Personen Ihres Vertrauens zur Verfügung. Wir empfehlen Ihnen, regelmäßig ein Backup Ihrer Daten anzulegen.

5. STARTEN SIE BEI VERBINDUNGSFEHLERN IHREN BROWSER ERNEUT
Bei auftretenden Verbindungsfehlern schließen Sie bitte den Browser und starten ihn erneut. Stellen Sie die korrekte Eingabe Ihrer entsprechenden Passwörter sicher. Schließen Sie bitte Ihren Browser nach Beenden der Internetsitzung.

6. SEIEN SIE VORSICHTIG BEI UNBEKANNTEN DATEIEN ODER EMAIL-ANHÄNGEN
Öffnen Sie keine Dateien unbekannter Herkunft oder Dateien, die Sie nicht angefordert haben.

7. BESUCHEN SIE KEINE WEBSEITEN MIT STRAFRECHTLICH RELEVANTEN INHALTEN
Dies gilt insbesondere für Seiten mit volksverhetzendem oder kinderpornographischem Inhalt, Seiten, die zu Straftaten anleiten oder Gewalt verherrlichen bzw. verharmlosen oder Seiten, die geeignet sind, Kinder oder Jugendliche sittlich schwer zu gefährden.

8. BETEILIGEN SIE SICH NICHT AN UNSERIÖSEN ODER RECHTSWIDRIGEN TAUSCHBÖRSEN
Beachten Sie beim Herunterladen oder Aufspielen von Dateien, insbesondere Musik, Filmen oder Bilder stets, dass diese urheberrechtlich geschützt sein können. Die Verletzung solcher Urheberrechte kann unter anderem erhebliche Schadensersatzansprüche gegen Sie auslösen.

9. VERFÜGBARKEIT, GEEIGNETHEIT ODER ZUVERLÄSSIGKEIT DES INTERNETZUGANGES
Wir geben keine Gewähr für die tatsächliche Verfügbarkeit, Geeignetheit oder Zuverlässigkeit des Internetzuganges für irgendeinen Zweck.

10. HAFTUNGSBESCHRÄNKUNG
Wir übernehmen keine Verantwortung für etwaige Schäden an Ihrem PC, die durch die Internetnutzung entstehen. Hiervon ausgenommen sind Schäden, zu denen wir vorsätzlich oder grob fahrlässig beigetragen haben. Insbesondere wird keinerlei Haftung für die Inhalte aufgerufener Websites oder heruntergeladener Dateien übernommen. Ferner wird auch keinerlei Haftung für einen etwaigen Virenbefall durch Verwendung des Internetzugangs übernommen.

11. HAFTUNGSFREISTELLUNG
Wir sind von sämtlichen Ansprüchen Dritter freizustellen, wenn unser Internetzugang von Ihnen rechtswidrig verwendet wird, insbesondere wenn Sie die oben stehenden Hinweise schuldhaft außer Acht gelassen haben.

12. DATENSCHUTZ
Soweit wir Ihre Daten im Rahmen der Internetnutzung über unseren Internetzugang erheben, werden diese selbstverständlich gemäß der geltenden Datenschutzbestimmungen behandelt.

13. BEI VERSTOSS GEGEN DIE NUTZUNGSHINWEISE
Sofern Sie gegen diese Nutzungshinweise verstoßen oder wir einen entsprechenden Verdacht haben, sehen wir uns gezwungen, Ihren Internetzugang einzuschränken oder zu sperren. Sollten Sie hierbei Daten verlieren, übernehmen wir dafür keine Haftung.

14. WEITERE HINWEISE
Die Nutzung unseres Internetzugangs ist auf die Dauer Ihrer Anwesenheit im Hotel beschränkt. Verbindung zum WLAN aufbauen („Hotel Tölzer Hof“): Die Nutzung erfolgt durch Eingabe eines Passwortes. Dieses darf nicht an Dritte weitergegeben werden.

Bei Fragen oder Problemen mit dem Internetzugang hilft Ihnen gerne unsere Rezeption. Wir empfehlen Ihnen für weitergehende Auskünfte die Seiten des Bundesamtes für Sicherheit in der Informationstechnik (www.bsi-fuer-buerger.de).