

Created by

(O)EBU

Hosted by

ORF

Host City

City of
Vienna

euRO ision
SONG CONTEST
VIENNA 2026

Hotel Awareness

HERBERT „HENK“ WAGNER | HEAD OF SECURITY
MARTIN PILS | HEAD OF CYBER SECURITY

Inhalt	1
Hotel Awareness.....	2
Sicherheit ist das Fundament unserer Gastfreundschaft.....	2
Teil 1: Physische Sicherheit.....	3
Teil 2: Hotel Awareness.....	4
Digitale Sicherheit.....	4
Management Checkliste - IT.....	5
Checkliste: Sicheres Hotel-Team	6
A) Allgemeine Sicherheit (Sicherheitstipps).....	6
B) Cybersecurity (The Secure 10).....	8

Sicherheit ist das Fundament unserer Gastfreundschaft

Liebe Partnerinnen und Partner der Wiener Hotellerie,

wir freuen uns sehr, den Eurovision Song Contest 2026 gemeinsam mit Ihnen auszurichten. Ob Sie tausende Fans willkommen heißen oder ein „Zuhause auf Zeit“ für eine der internationalen Delegationen sind: **Sie sind in diesen Wochen das Gesicht der Wiener Gastfreundschaft.**

Damit dieses Fest unbeschwert, offen und herzlich verläuft, möchten wir mit Ihnen einen Blick auf digitale Sicherheit und Diskretion werfen.

Wir sehen uns als ein Team – bestehend aus EBU, ORF, Stadt Wien, WienTourismus und der Polizei. Deshalb machen wir Ihnen als Partner keine komplizierten Vorschriften, sondern geben praktische „Tipps“ für den Alltag, um sich, Ihre Mitarbeitenden und besonders Ihre sensiblen Gäste zu schützen.

Status: Die Lage ist stabil. Lassen Sie sich von Schlagzeilen nicht verunsichern. Wir sind vorbereitet.

 Bundesministerium
Inneres



Vienna
12 POINTS



Teil 1: Physische Sicherheit

Aufmerksamkeit im gesamten Haus erhöhen

- **Einschleichdiebe** nutzen gezielt Trubel und Stoßzeiten. Achten Sie daher besonders in Stockwerken, Gängen, der Lobby und öffentlichen Bereichen auf hausfremde Personen.
- Lassen Sie Parkplätze, Freiflächen und Lieferzonen dabei nicht außer Acht.

Schlüssel- und Zutrittsmanagement konsequent umsetzen

- **Zentralschlüssel** sollten stets am Körper getragen werden (z.B. von Reinigungspersonal).
- Bei der Ausgabe von Schlüsseln oder Schlüsselkarten die **Identität des Gegenübers** **verlässlich prüfen**.
- **Nebeneingänge stets versperrt halten** (Notausgangsfunktion muss erhalten bleiben); Zutritt für Hausfremde über Seiteneingänge unterbinden.
- Geregelter Zutrittsprozedere für Lieferanten und Fremdfirmen definieren/umsetzen.
- Klare Regelungen für den Nachtzugang treffen und einhalten.

Check-in und Gästeregistrierung sorgfältig durchführen

- Führen Sie **Ausweiskontrollen ausnahmslos bei allen Gästen** durch
- **Umgang mit Gepäck und herrenlosen Gegenständen regeln**
- Versuchen Sie, herrenlose Gegenstände nach Möglichkeit einem Gast zuzuordnen.
- **Sprengstoffverdächtige Gepäckstücke nicht berühren** und sofort die Polizei verständigen.
- Vergessene Wertgegenstände wie Schlüssel, Laptops oder Brieftaschen dokumentiert verwahren.

Videoüberwachung und Technik prüfen

- Prüfen Sie bestehende Videoüberwachungsanlagen (und andere Sicherheitssysteme) regelmäßig auf Funktion und Aufzeichnung.

Bargeld und Betrugsversuche im Auge behalten

- Minimieren Sie Bargeldtransaktionen möglichst.
- Lassen Sie bei Bargeldzahlungen besondere Aufmerksamkeit walten (**Wechselbetrüger!**).
- Schöpfen Sie Bargeldbeträge regelmäßig ab und bringen Sie diese zur Bank.

Notfallorganisation sichtbar machen

- Hängen Sie Notrufnummern und interne Kontakte für Mitarbeitende aus.
- Definieren Sie Verantwortliche für Sicherheitsfragen.
- Halten Sie Evakuierungswege frei.

Gäste aktiv einbinden

Informationsblätter in Zimmern und an der Rezeption mit Hinweisen:

- Wertgegenstände nicht offen liegen lassen & Safe nutzen.
- Verdächtige Wahrnehmungen sofort melden.

Personal sensibilisieren und briefen

- Sicherheitsbriefings durchführen
- Mitarbeiter anhalten, verdächtige Beobachtungen sofort melden („see something, say something“)
- klare Ansprechpartner und Eskalationswege festlegen

Digitale Sicherheit

Der ESC ist ein weltweit beachtetes Großevent. Hotels geraten oft aus zwei Gründen ins Visier von digitalen Störfrieden:

1. **Störung (DDoS):** Angreifer versuchen, Webseiten durch künstliche Massenanfragen zu blockieren.
2. **Privatsphäre (Privacy):** Wenn Delegationen oder VIPs bei Ihnen wohnen, versuchen Dritte oft über den „Umweg Hotel“ an Informationen zu gelangen (Zimmernummern, Anwesenheit).

Sicherheitsstrategie: Maßnahmen für den Alltag

Sie müssen keine IT-Experten sein. Oft sind es die einfachen Verhaltensregeln im Team, die den größten Schutz bieten.

1. Digitale Diskretion: Das Smartphone bleibt privat

Ihre Mitarbeitenden sind zurecht stolz darauf, beim ESC dabei zu sein. In den sozialen Medien ist jedoch Vorsicht geboten.

- **Keine Fotos „hinter den Kulissen“:** Ein unbedachtes Selfie an der Rezeption, auf dem im Hintergrund ein Dienstplan, eine Gästeliste oder ein Ausweis (Badge) liegt, ist für Betrüger Gold wert.
- **Der „VIP-Radar“:** Schulen Sie Ihr Team darauf, keine Informationen über anwesende Delegationen auf Facebook, Instagram oder WhatsApp zu teilen. „Ratet mal, wer gerade eing_checked hat“ ist ein Sicherheitsrisiko.

2. Tricks am Telefon (Social Engineering)

Betrüger rufen oft an und geben sich als „ESC-Techniker“ oder „Management“ aus. Sie bauen Druck auf („Das Internet der Delegation muss sofort freigeschaltet werden!“, „Geben Sie mir schnell das WLAN-Passwort für Zimmer 304!“).

- **Unsere Bitte:** Seien Sie misstrauisch, wenn Anrufer Druck machen. Wir werden Sie niemals am Telefon nach Passwörtern fragen. Legen Sie auf und rufen Sie unter einer Ihnen bekannten Nummer zurück.

3. Technik sicher nutzen (WLAN & Drucker)

- **Das getrennte WLAN:** Lassen Sie Gäste (auch Delegationen) niemals in Ihr internes Hotel-Büro-Netzwerk. Nutzen Sie strikt getrennte Gäste-WLANs.
- **Sicheres Drucken:** Gästelisten oder Reisepass-Kopien dürfen nicht im Ausgabefach des Druckers liegen bleiben („Clean Desk“).

Management Checkliste - IT

Bitte gehen Sie diese Punkte einmalig mit Ihrem IT-Dienstleister durch.

THEMA	PRÜFUNG / MASSNAHME
DDoS-Schutz	Fragen Sie Ihren Provider: „Haben wir einen Basisschutz gegen Überlastung?“ (Oft Standard bei A1, Magenta, Cloudflare).
Netzwerk	Sind Gäste-WLAN und Hotel-Büro-WLAN strikt voneinander getrennt? Ein Gast darf nie auf interne PCs zugreifen.
Updates	Werden Rezeptions-Rechner regelmäßig neu gestartet (Updates)?
MFA	Ist für Booking-Plattformen und E-Mail die 2-Faktor-Authentifizierung aktiv?

Checkliste: Sicheres Hotel-Team

(O)EBU

ORF

City of
Vienna

EUROVISION
SONG CONTEST
VIENNA 2026

Zum Ausdrucken für Back-Office & Rezeption

A) Allgemeine Sicherheit (Sicherheitstipps)

Klare Abläufe gegen Diebstahl und unbefugten Zutritt.

Status	Regel
☐	Ausweiskontrolle: Ich kontrolliere Ausweise ausnahmslos bei allen Gästen.
☐	Schlüssel-Sicherheit: Ich trage Zentralschlüssel stets am Körper und gebe Schlüssel nur nach Identitätsprüfung aus.
☐	Zutrittskontrolle: Ich achte darauf, dass Nebeneingänge versperrt sind und lasse keine Hausfremden unkontrolliert ein.
☐	Wachsamkeit: Ich achte in Lobby und Gängen auf hausfremde Personen und melde verdächtige Beobachtungen sofort.
☐	Gepäck & Wertsachen: Ich lasse keine herrenlosen Gegenstände unbeachtet (Polizei bei Verdacht rufen!) und warne Gäste vor Taschendieben.
☐	Notfallplan für Offline Betrieb: Ich habe eine Kontaktliste und eine physische Buchungsliste für die Zeit der Veranstaltung vorbereitet.

Checkliste: Sicheres Hotel-Team

Ihr Kontakt zur Polizei: Die Telefonnummer 133

Achtung: Diese Kontaktnummer ist sowohl NOTRUF (bei Notfällen) als auch Ansprechstelle für anderweitige, polizeilich relevante Wahrnehmungen oder Hilfeersuchen.

Grundsätzlich gilt: „Lieber einmal zu viel anrufen, als einmal zu wenig.“

Einige konkrete Beispiele, wann „133“ als Kontakt zur Polizei angerufen werden kann/soll:

- Sicherheits-/kriminalpolizeiliche Vorfälle, die dringende Intervention erfordern, wie raufende Hotelgäste, Taschendiebstähle, Verdacht auf Betrugshandlungen, drohende Personen oder heftige Streitereien, Belästigungen, Verdacht auf falsche Ausweise oder Zahlungsmittel, Waffen, etc. (klassischer „Notruf“).
- Darüber hinaus können Sie unter „133“ aber auch relevante Wahrnehmungen melden, denen unter Umständen nachgegangen werden muss, z.B.: unbekannte Personen wollen sich Zutritt verschaffen oder einschleichen; jemand versucht, verdeckt oder durch Manipulation Daten oder Identitäten von und über Hotelgäste zu erlangen; in der Lobby befindet sich eine Person oder Personen, die keine Gäste sind und sich verdächtig verhalten; etc.
- Sonderfall „verdächtiger Gegenstand“: Es kommt laufend vor, dass herrenlose Koffer, Rucksäcke etc. aufgefunden und der Polizei gemeldet werden. Im hoteltechnischen Kontext sind derartige Gepäckstücke um ein Vielfaches wahrscheinlicher, weshalb es grundsätzlich wichtig ist, die Besitzer ausfindig zu machen, bevor ein Notruf getätigt wird.

Achtung: Sollte (aus welchen Gründen auch immer) das Gepäckstück als besonders verdächtig eingestuft werden, sollte umgehend 133 angerufen und der Sachverhalt gemeldet werden.

Checkliste: Sicheres Hotel-Team

ⓑ) Cybersecurity (The Secure 10)

Digitale Diskretion und Schutz vor Betrug.

Status	Regel
☐	Vorsicht am Telefon: Ich gebe am Telefon keine Passwörter, Zimmernummern oder VIP-Namen heraus. Bei Druck („Sofort!“) lege ich auf.
☐	Social Media: Ich poste keine Fotos aus dem Back-Office (Dienstpläne/Badges im Hintergrund) und keine Infos über anwesende Stars („VIP-Radar“).
☐	Netzwerk: Ich gebe Gästen niemals das Passwort für das interne Büro-WLAN.
☐	Clean Desk und Printer-Check: Ich sperre meinen PC (Windows+L), sobald ich aufstehe und lasse keine Pässe oder Listen im Drucker liegen.
☐	Phishing-Radar: Ich öffne keine Anhänge in E-Mails, die ich nicht erwarte oder die mich unter Druck setzen.
☐	USB-Tabu: Ich stecke keine fremden USB-Sticks an Hotel-PCs an.
☐	Digitales Schloss: Ich nutze die 2-Faktor-Anmeldung und teile mein Passwort nicht.
☐	Analoge Liste: Ich weiß, wo die gedruckte Notfall-Telefonliste liegt.
☐	Meldemut: Habe ich versehentlich etwas angeklickt? Ich melde es sofort („See something, say something“).
☐	Backup-Strategie: Funktioniert meine Backup-Strategie und wie lange ist mit der Wiederherstellung zu rechnen?

Checkliste: Sicheres Hotel-Team

(O)EBU

ORF

City of
Vienna

EUROVISION
SONG CONTEST
VIENNA 2026

Aktuelle Warnungen vor Online-Fallen listet die Watchlist Internet laufend auf ihrer Plattform www.watchlist-internet.at auf.

THEMA	ANSPRECHPARTNER	KONTAKT
Meldestelle Internetkriminalität	Bundeskriminalamt	against- cybercrime@bmi.gv.at
Cybercrime Helpline	Stadt Wien	Tel: 01 4000-4006

Interner Sicherheitsbeauftragter: _____