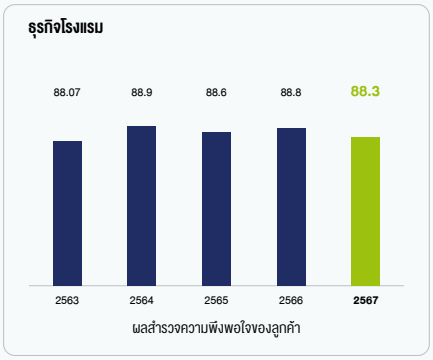
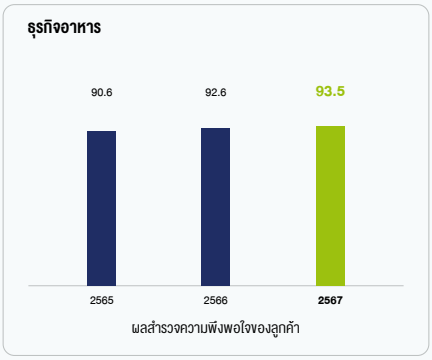
การประเมินความพึงพอใจของลูกค้าในการใช้บริการสำหรับธุรกิจอาหาร

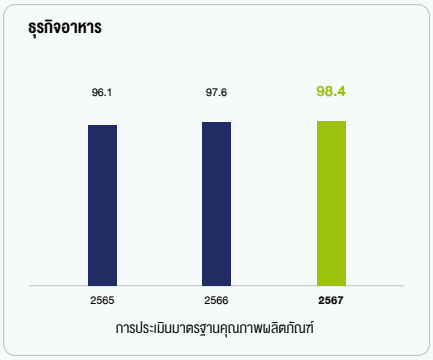
บริษัทได้นำแบบสำรวจความพึงพอใจลูกค้าออนไลน์ (Online Customer Questionnaires) มาใช้ควบคู่กับระบบตรวจสอบคุณภาพบริการจากมุมมองของลูกค้า (Mystery Shopping) เพื่อให้สามารถประเมินและวิเคราะห์ประสบการณ์ของลูกค้าได้อย่างครอบคลุมและแม่นยำ นอกจากนี้ บริษัทได้รวบรวมและติดตามข้อมูลผ่านระบบ CRG Food Tracker ซึ่งช่วยรวบรวมผลความพึงพอใจของลูกค้าและระบุประเด็นที่ต้องปรับปรุงได้อย่างเป็นระบบ ส่งผลให้การพัฒนาประสิทธิภาพการให้บริการเป็นไปอย่างรอบด้าน

ผลการประเมินความพึงพอใจของลูกค้าโดยรวมทุกแบรนด์

ในปี 2567 คะแนนความพึงพอใจของลูกค้าธุรกิจโรงแรมโดยรวมทุกแบรนด์ (Guest Satisfaction Survey Score : GSS) คือร้อยละ 88.3 ต่ำกว่าเป้าที่ตั้งไว้ร้อยละ 1 (เป้าร้อยละ 89.3) และคะแนนการจัดการชื่อเสียงในระบบออนไลน์ (Online Reputation Management Score: ORM) หรือ ดัชนีวัดความพึงพอใจของลูกค้า (Guest Review Index :GRI) คือร้อยละ 87.5 สูงกว่าค่าเฉลี่ยดัชนีวัดความพึงพอใจของโลกร้อยละ 1.3 แต่ยังต่ำกว่าเป้าที่ตั้งไว้ที่ร้อยละ 88.9 ในขณะที่คะแนนความพึงพอใจของลูกค้าในระหว่างการเข้าพักอยู่ที่ร้อนละ 86.3 สำหรับดัชนีความภักดีของลูกค้า (Net Promoter Score: NPS) สามารถทำ QCI ได้ 49 คะแนน เพิ่มขึ้นจากปีที่แล้ว 0.6 คะแนน โดยมีเป้าที่ 53 คะแนน ในส่วนผลคะแนนความสามารถในการแข่งขันเชิงคุณภาพการให้บริการ (Quality Competitive Index: CQI) คือ ร้อยละ 100.9 เทียบกับเป้าหมายที่ตั้งไว้ที่ร้อยละ 103.5







บริษัทได้ดำเนินการสรุปผลการสำรวจความพึงพอใจของลูกค้าและนำประเด็นสำคัญมาเป็นแนวทางในการพัฒนาและยกระดับคุณภาพการให้บริการ เพื่อให้สามารถตอบสนองความต้องการของลูกค้าได้ดียิ่งขึ้น ในการปรับปรุงด้านการให้บริการ บริษัทได้ดำเนินการพัฒนาความหลากหลายของเมนูอาหารในโรงแรมให้ครอบคลุมและตอบโจทย์ความต้องการของลูกค้าทุกกลุ่ม ในขณะเดียวกัน ยังคงให้ความสำคัญกับคุณค่าทางโภชนาการและความปลอดภัยของแหล่งที่มาของวัตถุดิบ เพื่อให้มั่นใจว่าอาหารที่ให้บริการมีคุณภาพและได้มาตรฐาน นอกจากนี้ บริษัทได้เพิ่มมาตรการตรวจสอบคุณภาพของห้องพักและพื้นที่ส่วนกลางของโรงแรมอย่างต่อเนื่อง เพื่อมอบประสบการณ์การเข้าพักที่สะดวกสบายและตรงตามความคาดหวังของลูกค้า รวมถึงการปรับปรุงฟังก์ชันของห้องพักให้สามารถรองรับการใช้งานอุปกรณ์อิเล็กทรอนิกส์ได้อย่างมีประสิทธิภาพและเพียงพอต่อความต้องการของผู้เข้าพัก

ในภาคธุรกิจอาหาร บริษัทได้กำหนดกรอบการดำเนินงานด้านคุณภาพการให้บริการ โดยแต่ละแบรนด์อาหารมีแนวปฏิบัติเฉพาะในการควบคุมคุณภาพ ซึ่งสะท้อนให้เห็นจากผลการประเมินความพึงพอใจของลูกค้าในปี 2567 โดยลูกค้ามีความพึงพอใจในด้านรสชาติและคุณภาพของอาหารที่เป็นไปตามมาตรฐาน รวมถึงความสะอาดและบรรยากาศโดยรวมภายในร้าน ผลการประเมินจากระบบ CRG Food Tracker พบว่าความพึงพอใจโดยรวมอยู่ที่ร้อยละ 93.5 และการประเมินมาตรฐานคุณภาพผลิตภัณฑ์อยู่ที่ร้อยละ 98.4 นอกจากนี้ บริษัทได้ให้ความสำคัญกับการพัฒนาคุณภาพในการให้บริการ 3 ประเด็นหลัก ได้แก่ ความรวดเร็วในการให้บริการ การเพิ่มเมนูและโปรโมชั่น และการต้อนรับลูกค้า เพื่อให้ตอบสนองความพึงพอใจลูกค้า บริษัทได้นำกลยุทธ์ด้านการดำเนินงานที่มุ่งเน้นการประยุกต์ใช้เทคโนโลยีเพื่อเพิ่มประสิทธิภาพการให้บริการ ควบคู่ไปกับการนำเสนอเซ็ตเมนูและโปรโมชั่นตามเทศกาลต่างๆ เพื่อเพิ่มยอดขายและขยายกลุ่มลูกค้าในตลาด

การคุ้มครองความเป็นส่วนตัวของข้อมูล

บริษัทได้จัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคล ตามข้อกำหนดของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และกฎหมายที่เกี่ยวข้องอย่างเคร่งครัด บริษัทตระหนักถึงความเสี่ยงด้านกฎระเบียบ (Compliance Risk) และความเสี่ยงจากการละเมิดสิทธิและความเป็นส่วนตัวของบุคคล จึงได้เผยแพร่ข้อมูลนโยบายดังกล่าวบนเว็ปไซต์ของบริษัท ทั้งเว็บไซต์ของธุรกิจโรงแรมและเว็บไซต์ของธุรกิจอาหาร รวมถึงสื่อความถึงลูกค้า คู่ค้า และผู้มีส่วนได้เสียทุกฝ่าย ให้รับทราบโดยทั่วกัน เพื่อสร้างความเชื่อมั่นในระบบการกำกับดูแลข้อมูลของบริษัท

บริษัทได้กำหนดให้มีการทบทวนนโยบาย แนวปฏิบัติ และปรับปรุงมาตรการการควบคุมข้อมูลให้เหมาะสมตามสถานการณ์ปัจจุบัน และได้จัดอบรมเพื่อให้ความรู้แก่พนักงานเกี่ยวกับความสำคัญของความเป็นส่วนตัวของข้อมูลและบทบาทขององค์กรในการรักษามาตรฐานของการรักษาความปลอดภัยและความเป็นส่วนตัวของข้อมูลของบริษัท โดยมีการดำเนินการอย่างสม่ำเสมอปีละหนึ่งครั้ง ในปี 2567 พนักงานได้เข้ารับการอบรมและผ่านการทดสอบ ร้อยละ 100

นอกจากนี้ บริษัทได้นำเทคโนโลยีที่มีประสิทธิภาพเข้ามาเสริมความแข็งแกร่งของระบบความมั่นคงปลอดภัยทางไซเบอร์ในการป้องกัน รักษาความปลอดภัยของระบบสารสนเทศและข้อมูลส่วนบุคคล เช่น การเลือกใช้ระบบการรักษาความปลอดภัยทางเครือข่าย (Firewall System) ระบบตรวจจับและตอบสนองต่อภัยคุกคามทางเครือข่าย (CrowdStrike) การยกระดับมาตรฐานการรักษาความปลอดภัยสำหรับการเข้าใช้งานระบบเทคโนโลยีสารสนเทศโดยวิธีการยืนยันตัวตนแบบหลายปัจจัย (Multi-factor Authentication : MFA) ที่มีความปลอดภัยสูง รวมถึงระบบการจัดการอุปกรณ์เคลื่อนที่ (Mobile Device Management : MDM) สำหรับบุคลากรที่เข้าถึงข้อมูลที่สำคัญ เป็นต้น ซึ่งเป็นส่วนช่วยในการสนับสนุนบริการและการดำเนินธุรกิจของบริษัท ด้านความโปร่งใสและการให้ความยินยอมเรื่องข้อมูล บริษัทได้สร้างช่องทางการสื่อสารที่ชัดเจนกับลูกค้า ผู้ใช้บริการ และผู้ที่เกี่ยวข้องกับการดำเนินธุรกิจ เพื่อขอความยินยอมที่สำคัญในการเก็บ ประมวลผล และแบ่งปันข้อมูล โดยได้กำหนดระเบียบปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล โดยกำกับดูแลให้มีการจัดเก็บข้อมูลเท่าที่จำเป็น ภายใต้วัตถุประสงค์อันชอบด้วยกฎหมาย นอกจากนี้ บริษัทจัดให้มีการดำเนินการตรวจสอบภายในรวมถึงหน่วยงานภายนอก โดยมีการตรวจสอบโดยเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของทางกลุ่มเซ็นทรัล

อ่านนโยบายความเป็นส่วนตัว เพิ่มเติม https://investor.centarahotelsresorts.com/th/privacy-policy

การบริหารความเสี่ยงด้านดิจิตอลและไซเบอร์ (Digital and Cyber Risk)

บริษัทให้ความสำคัญในการป้องกันและบริหารจัดการความเสี่ยงด้านดิจิตอลและไซเบอร์ให้สอดคล้องกับระดับความเสี่ยงที่องค์กรสามารถรับได้ คณะทำงานภายใต้การกำกับดูแลของประธานเจ้าหน้าที่ฝ่ายเทคโนโลยี จึงมุ่งมั่นในการปรับปรุงโครงสร้างทางด้านระบบเทคโนโลยีสารสนเทศให้มีปลอดภัยสูงสุด บริษัทมีแนวทางการทบทวนนโยบายอย่างสม่ำเสมอ อย่างน้อยปีละหนึ่งครั้ง และสร้างแผนรับรองเหตุการณ์ฉุกเฉินตามกระบวนการ CHR Crisis Escalation flow เพื่อใช้เป็นแนวทางในการสื่อสารและปฏิบัติภายในองค์กรให้สามารถจัดการความเสี่ยงได้อย่างมีประสิทธิภาพ เสริมด้วยการนำระบบการจัดการรักษาความปลอดภัยขององค์กร (Security Information and Event Management: SIEM) เพื่อจัดเก็บ ตรวจสอบหาจุดเสี่ยง วิเคราะห์ และระบุตำแหน่งของภัยคุกคาม โดยมีการดำเนินงานร่วมกับหน่วยงานภายนอก เพื่อยกระดับการเฝ้าระวังภัยคุกคามก่อนที่จะรบกวนการดำเนินธุรกิจ ภายในองค์กรเอง บริษัทจัดให้มีมาตรการควบคุมความปลอดภัยและความลับของข้อมูลตามมาตรฐานสากลและพึงคำนึงถึงสิทธิของลูกค้า รวมถึงผู้ที่มีส่วนเกี่ยวข้องทุกฝ่าย เพื่อคงไว้ซึ่งการรักษาความลับ (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) ของสารสนเทศ โดยมีการกำหนดระดับชั้นของข้อมูล เพื่อกำกับดูแลความปลอดภัยของข้อมูล นับตั้งแต่การบันทึกข้อมูล การเก็บและการใช้ข้อมูล และระยะเวลาในการเก็บรักษาข้อมูล โดยแต่ละหน่วยงานภายในบริษัทจะต้องรับผิดชอบการเก็บรักษา ดำเนินการลบ ทำลายหรือทำให้ข้อมูลส่วนบุคคลไม่สามารถระบุตัวตนได้

ในปี 2567 ธุรกิจโรงแรมและธุรกิจอาหารได้ดำเนินการทวนสอบระบบให้เป็นไปตามมาตรฐานและข้อกำหนดของการรับรองมาตรฐานการจัดการความปลอดภัยด้านสารสนเทศ (ISO/IEC 27001:2022 - Information Security Management) โดยหน่วยงานภายนอกเป็นที่เรียบร้อย

กระบวนการตรวจสอบระบบความปลอดภัยของข้อมูลสารสนเทศ (Cyber Security Incident Escalation)

บริษัทได้กำหนดมาตรการและขั้นตอนการตรวจสอบระบบความปลอดภัยของข้อมูลสารสนเทศอย่างเป็นระบบและรัดกุม เพื่อป้องกันและบริหารจัดการความเสี่ยงด้านไซเบอร์ รวมถึงการตอบสนองต่อภัยคุกคามที่อาจเกิดขึ้น ทั้งนี้ เพื่อให้ธุรกิจและการให้บริการสามารถดำเนินไปได้อย่างต่อเนื่อง บริษัทจึงได้กำหนดกระบวนการบริหารจัดการเหตุการณ์ด้านความปลอดภัยไซเบอร์ (Cyber Security Incident Management Procedure) และแผนการรับมือสถานการณ์ฉุกเฉิน (CHR Crisis Escalation Flow) ซึ่งมีการสื่อสารภายในองค์กรและทดสอบระบบเป็นระยะ นอกจากนี้ บริษัทให้ความสำคัญกับการส่งเสริมความร่วมมือกับหน่วยงานกำกับดูแลและภาคส่วนที่เกี่ยวข้อง เพื่อประสานงานด้านข้อมูลและระบบสารสนเทศให้เป็นไปตามข้อกำหนดทางกฎหมาย และสอดคล้องกับนโยบาย แนวปฏิบัติภายในองค์กรที่ได้มีการประกาศใช้

บุคลากรภายในบริษัทถือเป็นกลไกสำคัญในการเฝ้าระวังและรักษาความปลอดภัยของข้อมูลสารสนเทศ บริษัทจึงให้ความสำคัญกับการสร้างวัฒนธรรมองค์กรที่ตระหนักถึงความเสี่ยงด้านภัยไซเบอร์ในทุกระดับ ตั้งแต่คณะกรรมการบริษัท ผู้บริหาร พนักงาน ไปจนถึงลูกค้าและคู่ค้าที่เกี่ยวข้อง สำหรับระดับพนักงาน บริษัทได้จัดให้มีการฝึกอบรมด้านความเสี่ยงจากภัยไซเบอร์ รวมถึงการอบรมด้านกฎหมายคุ้มครองข้อมูลส่วนบุคคลเป็นประจำทุกปี พร้อมทั้งดำเนินโครงการทดสอบความตระหนักรู้ด้านภัยไซเบอร์ (Phishing Test) อย่างน้อยปีละสองครั้ง นอกจากนี้ บริษัทได้มีการตรวจสอบช่องโหว่ (Vulnerability Assessment) และจัดทำโครงการการทดสอบการบุกรุกระบบ (Cyber Security Penetration Test) ซึ่งได้ร่วมมือกับหน่วยงานภายนอกเพื่อประเมินความปลอดภัยทางไซเบอร์เสมือนจริงเป็นประจำในทุกปี ทั้งนี้ บริษัทได้กำหนดให้มีการรายงานสถานะของเหตุการณ์ด้านความเสี่ยงจากภัยไซเบอร์ ทั้งที่เกิดขึ้นภายในองค์กรและความเคลื่อนไหวจากภายนอกต่อผู้บริหาร เพื่อให้เกิดความตระหนักรู้และสามารถกำหนดแนวทางป้องกันที่มีประสิทธิภาพ ตลอดจนเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรให้สอดคล้องกับมาตรฐานสากล

บริษัทได้เข้าร่วมโครงการวัดระดับความมั่นคงปลอดภัยไซเบอร์สำหรับบริษัทจดทะเบียน (Cyber Resilience Survey 2025) ของตลาดหลักทรัพย์แห่งประเทศไทย เพื่อช่วยให้บริษัททราบถึงระดับความมั่นคงปลอดภัยไซเบอร์ของบริษัท และเป็นข้อมูลในการจัดทำแผนงานที่เกี่ยวข้องอันจะเป็นประโยชน์ในการลดความเสี่ยงและเพิ่มศักยภาพในด้านความมั่นคงปลอดภัยไซเบอร์ต่อไป