Ⅰ.ข้อมูลพื้นฐาน			
◆หัวข้อพื้นฐาน			
1	กฎหมายที่บังคับใช้เกี่ยวกับการบริการ	กฎหมายญี่ปุ่น	
2	กฎหมายที่ใช้บังคับเกี่ยวกับการปกป้องข้อมูลสำหรับบริการ	กฎหมายคุ้มครองข้อมูลส่วนบุคคล	
3	ความเป็นเจ้าของข้อมูลที่ลงทะเบียนในบริการ	ผู้ใช้บริการ	
4	องค์กรได้กำหนดนโยบายเกี่ยวกับความปลอดภัยของข้อมูลและการปกป้องข้อมูลส่วนบุคคลและมีการสื่อสารนโยบายเหล่านี้ทั้งภายในและภายนอกองค์กรหรือไม่	○	
5	บริษัทได้รับการรับรองจากบุคคลที่สามเกี่ยวกับความปลอดภัยของข้อมูลหรือการปกป้องข้อมูลส่วนบุคคลหรือไม่	○	・Privacy mark：Updated 2022 August 19 ・ISMS（ISO/IEC 27001）：Update 2022 March 23
6	องค์กรจัดระเบียบกฎหมาย ข้อบังคับ และข้อกำหนดตามสัญญาที่เกี่ยวข้องซึ่งผู้ให้บริการและบริการคลาวด์ต้องปฏิบัติตาม และองค์กรใช้ความพยายามอย่างต่อเนื่องเพื่อให้เป็นไปตามข้อกำหนดเหล่านี้หรือไม่	○	
7	หน่วยงานตรวจสอบภายนอกหรือแผนกประเมินผลอื่นๆ ประเมินเป็นประจำว่ามาตรการรักษาความปลอดภัยได้รับการปฏิบัติอย่างถูกต้องและดำเนินการตามที่ตั้งใจไว้หรือไม่ และเป็นไปตามกฎหมาย ข้อบังคับ และข้อกำหนดตามสัญญาที่เกี่ยวข้องหรือไม่	○	มีทำการตรวจสอบภายนอก
Ⅱ.หัวข้อเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล			
◆เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลและการใช้ข้อมูล			
8	นโยบายการคุ้มครองข้อมูลส่วนบุคคลมีการเปิดเผยต่อผู้ใช้บริการหรือไม่	○	
9	หากมีการบังคับใช้กฎหมายและข้อบังคับที่เกี่ยวข้องกับการปกป้องข้อมูลส่วนบุคคล สามารถปฏิบัติตามคำขอได้หรือไม่	○	
10	บริการเก็บรวบรวมข้อมูลส่วนบุคคลหรือไม่	○	
11	บริษัทใช้ข้อมูลส่วนบุคคลของผู้สมัครสมาชิกบริการหรือไม่	○	ข้อมูลของคุณจะไม่เปิดเผยชื่อและใช้เพื่อวัตถุประสงค์ทางการตลาด ฯลฯ
12	ข้อมูลส่วนบุคคลของผู้สมัครสมาชิกบริการถูกมอบให้กับบุคคลที่สามหรือไม่	×	
13	บริษัทของคุณใช้ข้อมูลที่ได้รับจากสมาชิกบริการหรือไม่	○	
14	ข้อมูลของผู้สมัครสมาชิกบริการนั้นมอบให้กับบุคคลที่สามหรือไม่	×	
15	ข้อมูลที่ได้รับจะถูกถ่ายโอนไปยังประเทศอื่นเนื่องจากการใช้บริการภายนอกหรือการจ้างภายนอกหรือไม่	×	
◆เกี่ยวกับข้อจำกัดความรับผิดชอบ			
16	มีมาตรฐานระดับการให้บริการหรือไม่	○	เราได้จัดทำ SLA อ้างอิง：https://h-t.co.th/assets/pdf/sla_th.pdf
17	มีเงื่อนไขของข้อสงวนสิทธิ์ในการใช้งานหรือไม่	○	กำหนดไว้ใน KING OF TIME หัวข้อที่ 12 อ้างอิง ：https://h-t.co.th/assets/pdf/term-of-use.pdf
Ⅲ.ความปลอดภัยทั่วไป			
◆เกี่ยวกับความปลอดภัยของข้อมูล			
18	มีการแต่งตั้งบุคคลให้รับผิดชอบด้านการจัดการความมั่นคงปลอดภัยของข้อมูล และได้กำหนดขอบเขต หน้าที่ อำนาจ และความรับผิดชอบแล้วหรือไม่	○	
19	ในส่วนของระบบการรักษาความมั่นคงปลอดภัยของข้อมูล ได้มีการกำหนดบทบาทหน้าที่ไม่เฉพาะเฉพาะเวลาปกติแต่ในกรณีฉุกเฉินด้วยหรือไม่	○	
20	ได้มีการชี้แจงแผนก ปฏิบัติการ และหน่วยงานที่เกี่ยวข้องกับการจัดการความปลอดภัยของข้อมูลแล้วหรือไม่	○	
21	บทบาทและความรับผิดชอบมีการกำหนดไว้อย่างชัดเจนโดยแยกส่วนที่จัดการภายในองค์กรและส่วนที่จะจ้างจากภายนอกอย่างเหมาะสมหรือไม่	○	
22	เพื่อลดความเสี่ยงของการเปลี่ยนแปลงโดยไม่ได้รับอนุญาตหรือไม่ได้ตั้งใจหรือการใช้งานโดยไม่ได้รับอนุญาต หน่วยงานในการเข้าถึง ดู และแก้ไขสินทรัพย์ข้อมูลแยกตามบทบาทและความรับผิดชอบขององค์กรหรือไม่	○	
23	เพื่อสร้างความตระหนักรู้เกี่ยวกับความปลอดภัยของข้อมูลและการจัดการข้อมูลที่สำคัญ จึงมีการศึกษาและการฝึกอบรมที่เหมาะสมเป็นประจำ และให้การศึกษาอย่างต่อเนื่องในกรณีที่ยังขาดความเข้าใจ	○	
◆มาตรการรักษาความปลอดภัยสำหรับพนักงาน			
24	พนักงานได้รับการศึกษาและการฝึกอบรมเพื่อเตรียมพร้อมสำหรับเหตุการณ์ด้านความปลอดภัยหรือไม่	○	
25	คุณได้สรุปข้อตกลงการรักษาความลับกับพนักงานของคุณหรือไม่	○	
26	เมื่อสัญญากับพนักงานและคู่ค้าสัญญาถูกยกเลิกหรือเปลี่ยนแปลง สิทธิ์การเข้าถึงมีการเปลี่ยนแปลงหรือถูกลบ และมีการส่งคืนสินทรัพย์ที่ยืมมาหรือไม่	○	

◆เกี่ยวกับการจัดการสินทรัพย์ข้อมูล			
27	คุณได้กำหนดกระบวนการและเกณฑ์การจัดการสำหรับความสำคัญของสินทรัพย์ข้อมูล ระบุและประเมินสินทรัพย์ข้อมูลตามกระบวนการจัดการ และสร้างรายการสินทรัพย์หรือไม่	○	
28	ได้ทำให้ไม่สามารถกู้คืนข้อมูลได้เมื่อลบสินทรัพย์ข้อมูลหรือserver หรือสื่อและcomponents ต่างๆหรือไม่	○	สื่อเก็บข้อมูลถูกทำลายทางกายภาพ
29	ในสัญญาการใช้บริการมีระบุไว้อย่างชัดเจนหรือไม่ว่าข้อมูลจะถูกจัดการอย่างไรเมื่อสิ้นสุดการให้บริการ	○	เมื่อคุณยกเลิกสัญญาเราจะทำการลบข้อมูลของคุณออก อย่างไรก็ตามเราจะไม่ลบออกจากข้อมูลbackupและจะencryptไว้
30	เมื่อสิ้นสุดการใช้บริการ ข้อมูลที่ได้รับความไว้วางใจจากผู้ใช้บริการหรือข้อมูลที่ผู้ใช้บริการสร้างขึ้นสามารถส่งคืนและลบได้หรือไม่	○	ไม่มีการส่งคืนข้อมูล แต่เราจะลบข้อมูลออก
◆Access Restrictions			
31	ได้มีการกำหนดขั้นตอนการจัดการเกี่ยวกับการจัดเก็บ การเคลื่อนย้าย การกำจัด และขอบเขตของผู้ใช้สื่อบันทึกข้อมูลภายนอก และสื่อที่ใช้เป็นไปตามขั้นตอนเหล่านั้นหรือไม่	×	ไม่ได้จัดเก็บไว้ในสื่อบันทึกข้อมูลภายนอก
32	นโยบายการควบคุมการเข้าถึงได้รับการกำหนดและปรับใช้สำหรับข้อมูลที่จัดการบนซอฟต์แวร์ ฮาร์ดแวร์ และเครือข่ายที่ใช้ในการพัฒนา บำรุงรักษา และการทำงานของบริการคลาวด์หรือไม่	○	
33	โดยหลักการแล้วพนักงานและผู้ดูแลระบบไม่ได้รับอนุญาตให้เข้าถึงข้อมูลที่ได้รับมอบหมายจากผู้ใช้บริการหรือไม่ เมื่อเข้าถึงข้อมูลที่ได้รับมอบหมายเมื่อจำเป็นเพื่อวัตถุประสงค์ทางธุรกิจ คุณจำกัดการเข้าถึงข้อมูลที่ได้รับการอนุมัติล่วงหน้าหรือไม่ และคุณตรวจสอบบันทึกการดำเนินการของผู้ที่เข้าถึงข้อมูลหรือไม่	○	การเข้าสู่ระบบของลูกค้าจะทำได้หลังจากได้รับอนุญาตเท่านั้น
34	การเข้าถึงcomponentsและข้อมูลภายในบริการคลาวด์นั้นจำกัดเฉพาะพนักงานที่ต้องการแต่ละcomponentsในการปฏิบัติหน้าที่หรือไม่	○	
35	การเข้าถึงเครือข่ายไปยังข้อมูลโดยใช้บัญชีพิเศษได้รับการบันทึกและตรวจสอบเพื่อให้แน่ใจว่ามีการใช้งานที่เหมาะสมหรือไม่	○	
36	สำหรับบริการคลาวด์ บัญชีที่ไม่จำเป็นหรือไม่ได้ใช้ในช่วงระยะเวลาหนึ่ง (รวมถึงการโอน การเลิกใช้งาน และการเปลี่ยนแปลงบทบาท) ถูกปิดใช้งานหรือลบหรือไม่	○	
37	โดยหลักการแล้ว ห้ามใช้บัญชีที่ใช้ร่วมกัน แต่ถึงแม้การใช้งานจะได้รับการอนุมัติในกรณีพิเศษ มีการตรวจสอบหรือไม่ว่าการใช้งานนั้นเหมาะสมหรือไม่โดยใช้บันทึกการจัดการ บันทึกการใช้งาน ฯลฯ (วิธีการยืนยันในส่วนหมายเหตุ)	○	
38	มีข้อกำหนดเฉพาะเพื่อป้องกันการออก ID ที่ออกซ้ำให้กับบุคคลอื่นหรือไม่	○	
39	เส้นทางการเชื่อมต่อถูกจำกัดโดยที่อยู่ IP ของแหล่งการเชื่อมต่อหรือไม่	○	สามารถจำกัดแหล่งการเชื่อมต่อของที่อยู่ IP ได้โดยการตั้งค่าที่มั่งลูกค้า
40	มีการใช้กลไกการตรวจสอบสิทธิ์ที่เหมาะสม เช่น การตรวจสอบสิทธิ์แบบหลายปัจจัย การลงชื่อเข้าระบบครั้งเดียว หรือการตรวจสอบสิทธิ์	○	
41	บัญชีที่ไม่ผ่านการเข้าใช้งานอย่างถูกต้องตามจำนวนที่ระบุจะถูกล็อคหรือห้ามไม่ให้เข้าใช้งานอีกในช่วงระยะเวลาหนึ่งหรือไม่	○	
42	การส่งข้อมูลมีการencryptedเมื่อทำการส่งหรือรับข้อมูลที่ได้รับการยืนยันแล้วหรือไม่	○	
43	หากไม่มีการดำเนินการภายในระยะเวลาหนึ่งหลังจากการเข้าสู่ระบบ เซสชันจะสิ้นสุดลงและมีการร้องขอการเข้าสู่ระบบอีกครั้งหรือไม่	○	ช่วงเวลาหมดอายุตั้งไว้ที่ 30 นาที
44	รหัสผ่านมีการกำหนดความซับซ้อนที่จำเป็นโดยแยกความแตกต่างระหว่างอักษรตัวพิมพ์ใหญ่และตัวพิมพ์เล็ก การรวมตัวอักษร ตัวเลข และอักขระพิเศษ และกำหนดจำนวนอักขระขั้นต่ำหรือไม่	○	
45	รหัสผ่านที่คุณป้อนไม่แสดงบนหน้าจอหรือไม่	○	
46	มีการจัดเก็บและส่งเฉพาะรหัสผ่านที่เข้ารหัสหรือไม่	○	
47	คุณได้กำหนดระยะเวลาหมดอายุรหัสผ่านขั้นต่ำและสูงสุดไว้หรือไม่	○	
48	ห้ามการใช้รหัสผ่านเดียวกันซ้ำข้ามรุ่นหรือไม่	○	
49	รหัสผ่านเริ่มต้นถูกใช้บนบริการบนคลาวด์serverและ components หรือไม่	○	
50	ผู้ใช้สามารถเปลี่ยนรหัสผ่านของตนเองได้หรือไม่	○	
51	เมื่อมอบหมายและใช้บัญชีสิทธิพิเศษในการพัฒนา การบำรุงรักษา และการดำเนินงานบริการคลาวด์ จำเป็นต้องได้รับการอนุมัติและจำกัดให้มีน้อยที่สุดหรือไม่	○	
52	สิทธิ์ของผู้ดูแลระบบและข้อจำกัดการเข้าถึงutilityที่มีสิทธิพิเศษมีไว้สำหรับบริการคลาวด์และแอปพลิเคชันหรือไม่	○	
53	บุคคลที่สามารถเข้าถึงแหล่งที่มาของโปรแกรม ข้อมูลจำเพาะ ฯลฯ ถูกจำกัดหรือไม่	○	
54	มีการควบคุมการเข้าถึงเพื่อจำกัดผู้ที่สามารถเผยแพร่หรือเริ่มการเปลี่ยนแปลงบริการคลาวด์ได้หรือไม่	○	
◆เกี่ยวกับข้อมูลและการencryption			
55	เพื่อปกป้องทรัพย์สินข้อมูล คุณมีนโยบายencryptionตามระดับความสำคัญและการใช้งานหรือไม่	○	
56	มีการควบคุมคีย์เข้ารหัสและรหัสผ่านเพื่อให้ผู้ดูแลระบบจำนวนจำกัดเท่านั้นที่สามารถเข้าถึงได้เมื่อจำเป็นหรือไม่	○	
57	ข้อมูลที่จัดเก็บไว้ในบริการถูกเข้ารหัสหรือปิดบังเพื่อไม่ให้รับรู้เนื้อหาข้อมูลเมื่อเข้าถึงฐานข้อมูลหรือไฟล์โดยตรงหรือไม่	○	
58	มีการควบคุมการเข้าถึงฐานข้อมูลและการตรวจสอบบันทึกการเข้าถึงหรือไม่	○	
59	ข้อมูลสำรองถูกเข้ารหัสเพื่อไม่ให้จดจำเนื้อหาได้หรือไม่	○	
60	มีการควบคุมการเข้าถึงข้อมูลสำรองและการตรวจสอบบันทึกการเข้าถึงหรือไม่	○	

61	เมื่อใช้การสื่อสารโดย SSL การสื่อสารโดยใช้โปรโตคอลการสื่อสารที่มีช่องโหว่ถูกห้ามหรือไม่	×	เครื่องลงเวลาบางส่วนใช้ TLS1.0 และ 1.1 ซึ่งขณะนี้เรามีแผนที่จะงดใช้
62	การสื่อสารได้รับการเข้ารหัสเมื่อเข้าถึงเว็บไซต์หรือไม่	○	
63	คุณใช้ใบรับรองเซิร์ฟเวอร์ SSL ที่ยังไม่หมดอายุและออกโดยผู้ออกใบรับรองที่เชื่อถือได้หรือไม่	○	เราใช้ใบรับรองเซิร์ฟเวอร์ SSL ที่ออกโดย GlobalSign
◆เกี่ยวกับความปลอดภัยทางกายภาพและสิ่งแวดล้อม			
64	ขอบเขตการรักษาความปลอดภัยทางกายภาพถูกกำหนดเพื่อปกป้องพื้นที่บางส่วนของข้อมูลและสิ่งอำนวยความสะดวกในการประมวลผลข้อมูลตามความสำคัญของสินทรัพย์ภายในขอบเขตหรือไม่	○	
65	การเข้าและออกจากพื้นที่รักษาความปลอดภัยได้รับอนุญาตตามการอนุมัติ และมีการควบคุมการเข้า/ออกโดยใช้การรับรองความถูกต้อง เช่น การรับรองความถูกต้องของบัตร IC หรือการรับรองความถูกต้องทางชีวภาพหรือไม่	○	
66	มีการตรวจสอบบันทึกการเข้า/ออกเป็นประจำเพื่อให้แน่ใจว่าไม่มีการเข้าถึงโดยไม่ได้รับอนุญาตหรือไม่	○	
67	มีมาตรการต่างๆ เช่น ติดตั้งกล้องวงจรปิดตามสถานที่สำคัญๆ และมีพยานร่วมด้วยหรือไม่	○	
68	ศูนย์ข้อมูลที่ใช้เป็นของในประเทศหรือไม่	○	
69	คุณใช้ภูมิภาคและศูนย์ข้อมูลในต่างประเทศหรือไม่	○	
◆เกี่ยวกับความปลอดภัยในการให้บริการ			
70	มีเอกสารกำกับเกี่ยวกับการกำหนดโครงสร้าง คุณสมบัติ ข้อกำหนด เงื่อนไขการให้บริการ และวิธีใช้งานของบริการคลาวด์หรือไม่	○	
71	สามารถเรียกดูการเปลี่ยนแปลงบริการคลาวด์ เพื่อตรวจสอบการเปลี่ยนแปลงที่ไม่ถูกต้อง และแสดงผลโครงสร้างระบบและเครือข่าย รวมถึงสถานะการเปลี่ยนแปลงได้หรือไม่	○	
72	มีการตรวจสอบฟังก์ชั่นและการทำงานของบริการคลาวด์เพื่อแก้ไขข้อบกพร่องอย่างสม่ำเสมอหรือไม่	○	
73	สามารถเรียกดูบันทึกการเปลี่ยนแปลงที่เกิดขึ้นในบริการคลาวด์ได้หรือไม่	○	
74	อนุญาตเฉพาะการเปลี่ยนแปลงที่ได้รับการอนุมัติแล้วเท่านั้นใช่หรือไม่	○	
75	มีการรายงานเกี่ยวกับข้อบกพร่องและการจัดการข้อบกพร่องตามวิธีการที่กำหนดสำหรับบริการคลาวด์หรือไม่	○	
76	มีการกำหนดระเบียบการแจ้งเตือนเกี่ยวกับการเปลี่ยนแปลงที่สำคัญหรือการยุติการให้บริการให้ผู้ใช้บริการทราบล่วงหน้าหรือไม่	○	
77	มีกำหนดเวลาการให้บริการและแจ้งให้ผู้ใช้บริการทราบหรือไม่	○	มีการแจ้งเตือนผ่านหน้าล็อกอินหรืออีเมล
78	มีการกำหนดระเบียบการแจ้งเตือนและเผยแพร่ข้อมูลเพิ่มเติมเมื่อเกิดเหตุขัดข้องหรือประสิทธิภาพในการให้บริการลดลงหรือไม่	○	มีการแจ้งเตือนผ่านหน้าล็อกอินหรืออีเมล
79	มีการกำหนดระเบียบการแจ้งเตือนในกรณีที่จำเป็นต้องบำรุงรักษาบริการคลาวด์อย่างเร่งด่วนให้ผู้ใช้บริการทราบล่วงหน้าหรือไม่	○	มีการแจ้งเตือนผ่านหน้าล็อกอินหรืออีเมล
80	มีการระบุเกี่ยวกับการจัดการข้อมูลไว้ในข้อตกลง สัญญา รวมถึงนโยบายการคุ้มครองข้อมูลส่วนบุคคล และเปิดเผยแก่ผู้ใช้บริการหรือไม่	○	
81	มีการจัดการแก้ไขปัญหาการขาดทรัพยากรอันเป็นผลมาจากการโจมตีโดยปฏิเสธการให้บริการ (DoS) หรือไม่	○	
82	มีการจัดการทรัพยากรโดยคำนึงถึงความต้องการในอนาคตด้วยหรือไม่	○	
83	มีการทดสอบในช่วงพัฒนาโดยตั้งค่าให้เหมือนกับสภาพการใช้งานจริงเพื่อป้องกันข้อบกพร่องที่อาจเกิดขึ้นจากการเปลี่ยนแปลงในสภาพการใช้งานจริงหรือไม่	○	
84	มีการติดตั้งซอฟต์แวร์ป้องกันมัลแวร์ในบริการคลาวด์ อุปกรณ์คอมพิวเตอร์ รวมถึงอุปกรณ์ที่ใช้สำหรับการให้บริการ และอัปเดตไฟล์รูปแบบมัลแวร์อย่างสม่ำเสมอหรือไม่	○	
85	เวลาของบริการคลาวด์ถูกจัดการให้ตรงกัน (ไทม์โซน) และมีการซิงค์เวลาโดยใช้ระบบเช่น NTP หรือไม่	○	
86	การติดตั้งและเปลี่ยนแปลงซอฟต์แวร์มีข้อจำกัดในการยืนยันอุปกรณ์ การยืนยัน MAC Address หรือการจำกัด IP Address ที่เชื่อมต่อหรือไม่	○	
◆เกี่ยวกับการสำรองข้อมูล			
87	มีการสำรองข้อมูลของบริการคลาวด์และข้อมูลการใช้งานเพื่อให้สามารถกู้คืนได้ในช่วงเวลาที่กำหนดหรือไม่	○	
88	มีการทดสอบการกู้คืนจากการสำรองข้อมูลเพื่อให้มั่นใจว่าสามารถกู้คืนได้อย่างถูกต้องหรือไม่	○	
89	มีการตรวจสอบว่าบริการคลาวด์มีการสำรองข้อมูลหรือไม่	○	ระบบจะทำการการสำรองข้อมูลจนถึง 04:00 น. ของวันก่อนหน้า
90	ข้อมูลสำรองของบริการคลาวด์ถูกจัดเก็บไว้ในภูมิภาคอื่นใช่หรือไม่	○	
◆การเก็บบันทึกข้อมูล			
91	มีการเก็บบันทึกเหตุการณ์และบันทึกการเข้าถึงที่บันทึกข้อผิดพลาดจากความขัดข้องของระบบ การจัดการข้อยกเว้น การทำผิดพลาด และเหตุการณ์ด้านความปลอดภัยหรือไม่	○	
92	มีการเก็บบันทึกการเข้าสู่ระบบและออกจากระบบของผู้ใช้งานและผู้ดูแลระบบหรือไม่	○	
93	มีการเก็บบันทึกการดำเนินการของผู้ใช้งานและผู้ดูแลระบบหรือไม่	○	
94	มีการกำหนดระยะเวลาการเก็บข้อมูลและบันทึก รวมถึงข้อกำหนดในการจัดการเพื่อให้สอดคล้องกับกฎหมายและระเบียบที่เกี่ยวข้องและดำเนินการตามกฎเหล่านั้นหรือไม่	○	
95	มีการจัดการระบบวิเคราะห์บันทึกของบริการคลาวด์อย่างมีประสิทธิภาพเพื่อให้สามารถวิเคราะห์เหตุการณ์ด้านความปลอดภัยได้ทันทีหรือไม่	○	
96	มีการป้องกันบันทึกและข้อมูลสำรองจากการเข้าถึงที่ไม่ถูกต้องและการปลอมแปลงผ่านการควบคุมการเข้าถึงและการเข้ารหัสหรือไม่	○	
◆เกี่ยวกับช่องโหว่ของระบบ			

97	มีการดำเนินการตรวจสอบช่องโหว่สำหรับบริการคลาวด์หรือไม่	○	มีการตรวจสอบแบบง่าย เช่น การสแกนพอร์ต และการตรวจสอบเชิงลึก เช่น การทดสอบการเจาะระบบทุกสัปดาห์
98	กรณีที่มีการเปลี่ยนแปลงโครงสร้างพื้นฐาน เครือข่าย หรือการดำเนินการของบริการคลาวด์ ได้ทำการตรวจสอบช่องโหว่ทั้งในด้านฟังก์ชันและด้านความปลอดภัย และตรวจสอบว่าไม่มีผลกระทบหรือข้อบกพร่องหลังการเปลี่ยนแปลงหรือไม่	○	
99	มีการตรวจสอบช่องโหว่ก่อนการเปลี่ยนแปลงบริการคลาวด์ และดำเนินมาตรการตามผลการตรวจสอบหรือไม่	○	มีการตรวจสอบช่องโหว่โดยองค์กร/หน่วยงานตรวจสอบเฉพาะทางอย่างน้อยปีละหนึ่งครั้ง รวมถึงก่อนการเปิดใช้บริการและหลังการแก้ไข/เปลี่ยนแปลง (Webแอปพลิเคชั่น เครือข่าย แอปพลิเคชันบนสมาร์ทโฟน ฯลฯ) หรือไม่
100	มีการรวบรวมข้อมูลเกี่ยวกับช่องโหว่และการสิ้นสุดการสนับสนุน (EOSL) ของระบบปฏิบัติการ ซอฟต์แวร์ และการอัปเดตแพตช์สำหรับบริการคลาวด์อย่างสม่ำเสมอหรือไม่	○	
101	มีการกำหนดนโยบายในการจัดการช่องโหว่ตามระดับความเสี่ยงและระยะเวลาในการจัดการตามระดับความเสี่ยงนั้น และดำเนินการตามนโยบายหรือไม่	○	
◆เกี่ยวกับเหตุการณ์ด้านความปลอดภัย			
102	มีการกำหนดขั้นตอนการจัดการเหตุการณ์ด้านความปลอดภัยและความขัดข้องของระบบหรือไม่	○	
103	มีการตรวจสอบประสิทธิภาพของบริการคลาวด์และเครือข่ายเพื่อการตรวจจับเหตุการณ์ด้านความปลอดภัยและความขัดข้องของระบบหรือไม่	○	
104	มีการตรวจสอบการทำงานและการเฝ้าระวังปัญหาการใช้งาน (การเฝ้าระวังจากภายนอก) เพื่อการตรวจจับเหตุการณ์ด้านความปลอดภัยและความขัดข้องของระบบหรือไม่	○	
105	มีการเฝ้าระวังการเข้าถึงและการใช้งานที่ไม่ได้รับอนุญาตทั้งจากภายในและภายนอกเพื่อการตรวจจับเหตุการณ์ด้านความปลอดภัยและความขัดข้องของระบบหรือไม่	○	
106	มีการเฝ้าระวังแพ็กเก็ตที่มีรูปแบบไม่ถูกต้องเพื่อตรวจจับเหตุการณ์ด้านความปลอดภัยและความขัดข้องของระบบหรือไม่	○	
107	มีการเฝ้าระวังการเข้าถึงเครือข่ายที่ไม่ได้รับอนุญาตและการเข้าถึงจากระยะไกลเพื่อตรวจจับเหตุการณ์ด้านความปลอดภัยและความขัดข้องของระบบหรือไม่	○	
108	มีการระบุความรับผิดชอบและบทบาทหน้าที่อย่างชัดเจนเพื่อการตอบสนองต่อเหตุการณ์ด้านความปลอดภัยและความขัดข้องของระบบอย่างรวดเร็วและมีประสิทธิภาพหรือไม่	○	
109	มีการจัดทำแผนการฟื้นฟูและแผนการตอบสนองฉุกเฉินเพื่อเตรียมพร้อมสำหรับเหตุภัยพิบัติ เช่น แผ่นดินไหว ไฟไหม้ หรือความขัดข้องของระบบขนาดใหญ่หรือไม่	○	
110	มีการกำหนดขอบเขตของเหตุการณ์ด้านความปลอดภัยและกำหนดขั้นตอนการแจ้งเตือนแก่ผู้ใช้บริการอย่างชัดเจนหรือไม่	○	กรณีที่มีข้อมูลส่วนบุคคลของลูกค้ารั่วไหล สูญหาย หรือเกิดความเสียหาย จะมีการแจ้งให้ทราบผ่านทางอีเมลและหน้าเว็บไซต์ทันที พร้อมกับแจ้งรายงานการสอบสวนอย่างเร็วที่สุด
◆เกี่ยวกับความปลอดภัยของเครือข่าย			
111	มีการอนุญาตการเข้าถึงบริการคลาวด์จากระยะไกลโดยที่ต้องได้รับอนุญาตจากผู้ดูแลระบบก่อนหรือไม่	○	
112	มีการติดตั้งไฟร์วอลล์เพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตจากทั้งภายนอกและภายในหรือไม่	○	
113	มีการอัปเดตไฟล์รูปแบบและคำจำกัดความของอุปกรณ์ป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตอยู่เป็นประจำหรือไม่	○	
114	มีการติดตั้ง WAF เพื่อป้องกันการโจมตีที่ใช้ช่องโหว่ของเว็บแอปพลิเคชันหรือไม่ ※ WAF …Web Application Firewall	○	
115	มีการอัปเดตไฟล์รูปแบบและคำจำกัดความของ WAF อยู่เป็นประจำหรือไม่ ※ WAF … Web Application Firewall	○	
116	มีมาตรการรับมือ/ป้องกันการโจมตีที่ขัดขวางการดำเนินการ เช่น DDoS หรือไม่ ※ DDoS … Distributed Denial of Service attack	○	
117	มีการอัปเดตไฟล์รูปแบบและคำจำกัดความสำหรับการป้องกันการขัดขวางการดำเนินการอยู่เป็นประจำหรือไม่	○	
118	ในกรณีที่ตรวจพบการเข้าถึงที่ไม่ได้รับอนุญาต มีการกำหนดขั้นตอนการแจ้งเตือนให้ผู้ดูแลระบบและผู้ใช้งานระบบทราบทันทีหรือไม่	○	
119	กรณีที่บริษัทที่ใช้บริการเข้าถึงบริการคลาวด์ สามารถจำกัดเส้นทางการเชื่อมต่อตาม IP Address ของต้นทางได้หรือไม่	○	
120	กรณีที่เข้าถึงหน้าจอการจัดการที่ใช้ในการพัฒนาและบำรุงรักษาบริการคลาวด์ สามารถจำกัดเส้นทางการเชื่อมต่อตาม IP Address ของต้นทางได้หรือไม่	○	
121	ในบริการคลาวด์ มีการป้องกันขอบเขตด้วยการแยกเชิงตรรกะตามการใช้งานของแต่ละเซิร์ฟเวอร์หรือไม่	○	
122	มีการแยก DBเซิร์ฟเวอร์และ Webเซิร์ฟเวอร์ ออกจากกัน และควบคุมการเข้าถึงเพื่อให้การสื่อสารระหว่าง Webเซิร์ฟเวอร์และ DBเซิร์ฟเวอร์อยู่ในระดับต่ำที่สุดหรือไม่	○	
123	มีการควบคุมการเข้าถึงเพื่อไม่ให้สามารถเข้าถึง DBเซิร์ฟเวอร์ได้โดยตรงจากภายนอกหรือไม่	○	

124	การรับส่งข้อมูลบนบริการคลาวด์ มีการใช้การเข้ารหัสหรือเซ็ตติจิตเพื่อรักษาความลับและความครบถ้วนของข้อมูลในเส้นทางการส่งข้อมูลหรือไม่	○	
◆เกี่ยวกับการพัฒนา และการบำรุงรักษาระบบบริการคลาวด์			
125	ในการพัฒนาและการบำรุงรักษาบริการคลาวด์ มีการกำหนดข้อกำหนดด้านความปลอดภัยอย่างชัดเจนหรือไม่	○	
126	มีการระบุและตรวจทานข้อกำหนดด้านฟังก์ชันการใช้งาน (Functional requirememt และ Non-functional requirement) และข้อกำหนดด้านความปลอดภัยในแต่ละขั้นตอนของการพัฒนา การบำรุงรักษา และการดำเนินการเพื่อคำนึงถึงความปลอดภัยและคุณภาพหรือไม่	○	
127	มีการตรวจทานการเขียนโค้ดอย่างปลอดภัยและทดสอบความปลอดภัยในแต่ละขั้นตอนของการพัฒนา การบำรุงรักษา และการดำเนินการหรือไม่	○	
128	มีการจัดทำกระบวนการอนุมัติและกระบวนการแก้ไขข้อมูลในแต่ละขั้นตอนของการพัฒนา การบำรุงรักษา และการดำเนินการหรือไม่	○	
129	มีการแยกสภาพแวดล้อมการพัฒนาออกจากสภาพแวดล้อมการใช้งานจริงเพื่อป้องกันการรั่วไหลของข้อมูลในระหว่างการพัฒนา การบำรุงรักษา และการดำเนินงานหรือไม่	○	
130	มีการห้ามทำซ้ำหรือใช้ข้อมูลสภาพแวดล้อมการใช้งานจริงในสภาพแวดล้อมอื่น ๆ (เช่น การใช้งานในการทดสอบ) เพื่อป้องกันการรั่วไหลของข้อมูลในระหว่างการพัฒนา การบำรุงรักษา และการดำเนินงานหรือไม่	○	
131	มีการจำกัดและตรวจสอบเพื่อไม่ให้มีการใช้งานซอฟต์แวร์ที่ห้ามใช้บนอุปกรณ์ที่ใช้ในการพัฒนาและบำรุงรักษาบริการคลาวด์หรือไม่	○	
132	เมื่อมีการเปลี่ยนแปลงแอปพลิเคชัน มีการทดสอบและยืนยันล่วงหน้าเพื่อดูผลกระทบและข้อผิดพลาดหรือไม่	○	
◆เกี่ยวกับจัดจ้างงานบริการจากภายนอก			
133	มีการให้บริษัทเอาท์ซอร์สใช้งานข้อมูลที่รับฝากในระบบหรือไม่	○	มีการใช้ในงานสนับสนุนและงานตรวจสอบข้อผิดพลาดตามความจำเป็น
134	มีการเรียกร้องและทำข้อตกลงกับบริษัทเอาท์ซอร์สให้มีมาตรฐานความปลอดภัยทางข้อมูลเทียบเท่ากับของบริษัทหรือไม่	○	
135	มีการประเมินบริษัทเอาท์ซอร์สอยู่เป็นประจำหรือไม่	○	ดำเนินการปีละ 1 ครั้ง