



ניהול המשכיות עסקית

פרק א' - כללי

מבוא

1. חוק נתוני אשראי, תשע"ו-2016 (להלן - "החוק") הסמיך את הממונה על שיתוף בנתוני אשראי לקבוע הוראות בעניינים שונים הנוגעים לפעילותן של לשכות אשראי, בין היתר, בנוגע לניהולן התקין של הלשכות. ניהול תקין כולל בחובו, בין היתר, ניהול המשכיות עסקית.
2. מתוקף סמכותי לפי סעיף 68 לחוק נתוני אשראי, ולאחר התייעצות בוועדה המייעצת, הריני קובע הוראה זו. מטרת ההוראה לקבוע עקרונות של מסגרת עבודה לניהול המשכיות עסקית בלשכות אשראי. זאת לצורך חיזוק עמידותן בעת התרחשות שיבושים תפעוליים משמעותיים הנגרמים מאירועים חיצוניים או פנימיים ללשכה ושיפור יכולתן לנהל אירועי התאוששות ממצב חירום באופן מיטבי, לרבות הקטנת הנזקים ששיבושים מסוג זה עלולים לגרום לרציפות הפעילות העסקית, לאספקת שירותים לציבור, למוניטין ולרווחיות, ובאופן שיאפשר להן לעמוד בהוראות הדין החלות עליהן.
3. סיכוני המשכיות עסקית מהווים חלק מניהול הסיכון התפעולי ולפיכך, בכל הנוגע לניהול המשכיות עסקית, הוראה זו מוסיפה על הוראה 303 בנושא ניהול סיכונים.

תחולה

4. הוראה זו חלה על לשכת אשראי.
5. הממונה רשאי לפטור לשכת אשראי מסוימת מקיום סעיפים מסוימים בהוראה זו או לקבוע הוראות מסוימות שונות מאלו המפורטות להלן אשר יחולו על לשכת אשראי מסוימת. זאת, במקרים חריגים לאחר שבחן את בקשתה ונימוקה, אשר נמסרו לו בכתב, ורשאי הממונה לקבוע כי הפטור או ההוראות השונות יחולו לתקופה קצובה כפי שתיקבע על ידו.

הגדרות

6. בהוראה זו –

אתר המוחזק במצב של מוכנות ומיועד לשימוש על מנת לשמור על הרציפות העסקית של הלשכה, לרבות מרחב העבודה, מערכות המידע ואישוש הנתונים;	-	"אתר חלופי" DR- (Disaster Recovery Site/Alternate site)
אתר ראשי ואתר חלופי;	-	"אתר קריטי"
אתר המשמש את הלשכה לפעילותה השוטפת במצב עסקים רגיל, לרבות מרחב העבודה ומערכות המידע;	-	"אתר ראשי"
הוראת הממונה מס' 301 בנושא ניהול המידע והגנתו;	-	"הוראה 301 בנושא ניהול המידע והגנתו"



	- הוראה 303 בנושא ניהול סיכונים	הוראת הממונה מס' 303 בנושא ניהול סיכונים ;
	- "המשכיות עסקית" (Business continuity)	מצב בו עסק פועל ברציפות ללא הפרעות ;
	- "התאוששות" (Recovery)	שיקום פעולות עסקיות מסוימות לאחר שחל שיבוש באותן פעולות, עד לרמה מספקת לצורך מילוי ההתחייבויות העסקיות ;
	- "זמן התאוששות" (Recovery Time)	פרק הזמן שהוגדר להחזרת פעולה עסקית מסוימת לפעילות והוא כולל שני מרכיבים: משך הזמן החולף מתחילת השיבושים ועד להפעלת תוכנית ההמשכיות העסקית וכן משך הזמן מתחילת הפעלת תוכנית ההמשכיות העסקית עד להתאוששות של פעולה עסקית מסוימת. זמן ההתאוששות מהווה מרכיב של יעד ההתאוששות ;
	- "יעד גיבוי הנתונים" (Recovery Point Objective - RPO)	התדירות המינימלית שהוגדרה מראש, לגיבוי הנתונים הנדרשים להתאוששות, קרי, היקף המידע המקסימלי במונחי זמן שהלשכה תהיה מוכנה "לאבד" בעת שיבוש תפעולי משמעותי ;
	- "יעד התאוששות" (Recovery Time Objective - RTO)	יעד, מוגדר מראש, להחזרת תהליכים ושירותים חיוניים, עד לרמת שירות שהוגדרה להתאוששות (רמת שירות להתאוששות) ובמסגרת זמן ההתאוששות ;
	- "מערכות מידע"	כהגדרתן בהוראה 301 בנושא ניהול המידע והגנתו ;
	- "ניהול המשכיות עסקית" (Business Continuity Management)	גישה כלל-ארגונית הכוללת קווי מדיניות, ונהלים שתכליתם לוודא כי ניתן יהיה לבצע פעולות מסוימות או להשיבן לפעילות במועד, במקרה של שיבושים תפעוליים משמעותיים ;
	- "עמידות" (Resilience)	היכולת של לשכה לספוג את השלכותיו של שיבוש תפעולי משמעותי, ולהמשיך ולנהל תהליכים ושירותים חיוניים ;
	- "רמת שירות להתאוששות" (Recovery Level)	רמת השירות האלטרנטיבית שהוגדרה מראש כיעד אשר יסופק בנוגע לפעולה עסקית מסוימת לאחר שחל שיבוש בפעילות תפעולית משמעותית. רמת שירות להתאוששות מהווה מרכיב של יעד ההתאוששות ;



<p>- שיבוש בעל השפעה חמורה על הפעילות העסקית הרגילה, לדוגמה: הרס או פגיעה חמורה בתשתית פיזית, במתקנים או במערכות מידע, אובדן או אי נגישות של כוח אדם ונגישות מוגבלת לאזור שנפגע. שיבוש תפעולי משמעותי עלול להיגרם ממגוון רחב של אירועים כגון:</p> <p>- אירועים שהמדינה נדרשת אליהם ברמה הלאומית (להלן- "אירועים לאומיים") כגון: מלחמה, מתקפות טרור, רעידות אדמה, אירועים הקשורים למזג האוויר, מגיפה ואירועים ביולוגיים אחרים העלולים לגרום להדבקת עובדים ובידוד עובדים לתקופה ממושכת, או אירוע אחר בו מתקיים מצב של "שעת חירום";</p> <p>- אירועים פנים ארגוניים, כגון: שריפה, אירוע סייבר או אירועים אחרים הגורמים נזק רחב לתשתית הפיזית או למערכות המידע;</p>	<p>"שיבוש תפעולי משמעותי" (Major operational disruption) / "מצב חירום"</p>
<p>- כל אחד מאלה:</p> <p>(1) תקופת הפעלת מערך משק לשעת חירום בהתאם להחלטת הממשלה מס' 1716 מיום כ"ט בסיון התשמ"ו, 6 ביולי 1986 ולהחלטת ממשלה מס' 1080 מיום ז' באדר א' התש"ס, 13 בפברואר 2000, וכל החלטת ממשלה אחרת בעניין;</p> <p>(2) הכרזה על מצב מיוחד בעורף לפי סעיף 9 לחוק התגוננות אזרחית תשי"א-1951;</p> <p>(3) הכרזה על אירוע חירום אזרחי לפי סעיף 90 לפקודת המשטרה [נוסח חדש], התשל"א-1971;</p> <p>(4) הכרזה על מחלה מידבקת מסוכנת לפי פקודת בריאות העם, 1940.</p>	<p>"שעת חירום"</p>
<p>- כל פעילות, פונקציה, תהליך או שירות שהם חיוניים לשמירה על יציבותה והמשך רציפות פעילותה של הלשכה, לרבות מתן שירותים לנותני האשראי ושמירה על עניינם של לקוחות, וכן לאמון הציבור בה.</p>	<p>"תהליך או שירות חיוני" (Critical operation or service)</p>
<p>- תוכנית פעולה מקיפה בכתב, הקובעת מה הם הנהלים והמערכות הדרושים כדי לשמר את הרציפות העסקית או לשקם את פעילות הלשכה במקרה של שיבושים תפעולים משמעותיים.</p>	<p>"תוכנית עסקית" (Business Continuity Plan)</p>
<p>- מכלול אירועים לאומיים ופנים ארגוניים שעלולים לגרום לשיבוש תפעולי משמעותי של הלשכה.</p>	<p>"תרחישי ייחוס"</p>



פרק ב' - ממשל תאגידי

כללי

7. הדירקטוריון וההנהלה יהיו אחראים לקיומה של מסגרת עבודה הולמת לניהול המשכיות עסקית של הלשכה, ובין השאר, ינחילו תרבות אירגונית שיש בה מוכנות להמשכיות עסקית המוטמעת בתהליכי ניהול הסיכונים השוטפים.

הדירקטוריון

8. הדירקטוריון יתווה את מסגרת העבודה לניהול המשכיות עסקית (להלן – "מסגרת העבודה") וכן ידון ויאשר אותה, לכל הפחות אחת לשנה ובעת שינוי מהותי בסביבת הפעילות ובחשיפה לסיכונים. מסגרת העבודה תכלול, בין השאר, מדיניות לניהול המשכיות עסקית ותוכנית המשכיות עסקית כמפורט בהוראה זו.
9. בדיון על מסגרת העבודה, הדירקטוריון ידון, בין היתר, באפקטיביות מסגרת העבודה לרבות קיום פיקוח נאות על יישומה על ידי ההנהלה.
10. הדירקטוריון ידון, לכל הפחות, אחת לשנה, בתוצאות התרגולים שנערכו בלשכה, בהתאם לתוכנית התרגולים השנתית שנקבעה על ידי ההנהלה.

ההנהלה

11. ההנהלה נושאת באחריות ליישום מסגרת העבודה להמשכיות עסקית. תפקידה כולל, בין היתר, גיבוש מסמך מדיניות ותוכנית המשכיות עסקית והטמעתם בתהליכי ניהול הסיכונים בלשכה, וזאת על מנת לוודא כי סיכוני המשכיות עסקית מנוהלים באופן ראוי.
12. ההנהלה תמנה אחראי המשכיות עסקית ותגדיר את תחומי אחריותו וסמכויותיו. אחראי המשכיות העסקית יכול להיות בעל תפקידים נוספים בלשכה, ובלבד שלא יהיו בתפקידיו הנוספים כדי לפגוע ביכולתו לנהל את המשכיות העסקית בלשכה כראוי.
13. ההנהלה תמנה צוות לניהול משבר ותגדיר את תפקידו במצב חירום, כמפורט בפרק ה'. הצוות יכלול מקבלי החלטות מרכזיים וגורמים מקצועיים, באופן שיבטיח ניהול מיטבי של המשבר ויכולת קבלת החלטות במצבי לחץ. הצוות יורכב, בין היתר, מהגורמים הבאים: מנכ"ל הלשכה; מנהל הסיכונים; אחראי המשכיות עסקית והממונה על אבטחת מידע.
14. ההנהלה, באישור הדירקטוריון, תקצה משאבים נאותים ליישום והטמעת תוכנית המשכיות העסקית.
15. ההנהלה תדווח באופן מידי לדירקטוריון במקרה של אירוע התממשות סיכון תפעולי משמעותי בנושא המשכיות העסקית או כל אירוע כאמור שכמעט והתרחש.

פרק ג' - דיווחים לממונה

16. הלשכה תדווח לממונה במקרה של אירוע התממשות סיכון תפעולי משמעותי בנושא המשכיות עסקית או כל אירוע כאמור שכמעט והתרחש, בהתאם למפורט בסעיפים 27 ו-28 להוראה 303 בנושא ניהול סיכונים.



פרק ד' - מדיניות לניהול המשכיות עסקית

17. ההנהלה תגבש מסמך מדיניות לניהול המשכיות עסקית ותביאו לאישור הדירקטוריון. ההנהלה תבחן את הצורך בעדכון מסמך המדיניות, לכל הפחות אחת לשנה ובעת שינוי מהותי בסביבת הפעילות ובחשיפה לסיכונים, ותעביר המלצותיה לדירקטוריון.
18. מסמך המדיניות לניהול המשכיות עסקית יכלול, בין היתר, את המרכיבים הבאים :
- 18.1. **ניתוח השלכות עסקיות (BIA- Business Impact Analysis)** הבנוי משני שלבים :
- 18.1.1. ניתוח תרחישי ייחוס הרלוונטיים להמשכיות עסקית והערכת מכלול הסיכונים אשר עלולים להשפיע על המשכיות העסקית של הלשכה כתוצאה משיבוש תפעולי משמעותי ;
- 18.1.2. זיהוי התהליכים והשירותים החיוניים וניתוח ההשלכות העסקיות (כספיות, תדמיתיות, גולטריות, משפטיות וכיו"ב) כתוצאה מאי זמינות של תהליכים ושירותים חיוניים ללשכה בכל אחד מתרחישי הייחוס הרלוונטיים.
- 18.2. **אסטרטגיית ההתאוששות** - הגדרת המענה הנדרש להתאוששות התהליכים והשירותים החיוניים, על מנת לעמוד ביעדי גיבוי הנתונים ויעדי ההתאוששות שהוגדרו עבור כל אחד מהתהליכים והשירותים החיוניים. הגדרת יעדי גיבוי נתונים ויעדי התאוששות אלו תתבצע בהתאם לניתוח ההשלכות העסקיות. יעדי ההתאוששות שיקבעו למתן השירותים הבאים על ידי הלשכה ללקוחותיה לא יעלו על שעות ספורות ממועד תחילת השיבושים :
- 18.2.1. מסירת דוח אשראי או דוח ריכוז נתונים לפי החוק ;
- 18.2.2. מסירת חיווי אשראי לנותן אשראי לפי החוק ;
- 18.2.3. ביצוע דירוג אשראי ומסירתו לנותן אשראי לפי החוק.
- ככל וקיים פער בין יכולת ההתאוששות הקיימת בלשכה לבין יעדי גיבוי הנתונים ויעדי ההתאוששות שנקבעו, על הלשכה להגדיר את אופן הטיפול בפער זה.
- 18.3. **תוכנית המשכיות עסקית** - קביעת הנחיות מפורטות ליישום אסטרטגיית ההתאוששות, כמפורט בפרק ה'.
- 18.4. **ניטור סיכונים, הטמעת תוכנית המשכיות עסקית וקביעת תוכנית תרגולים** - הטמעת תוכנית המשכיות העסקית בקרב עובדיה של הלשכה, וכן ניטור ותיקוף התוכנית בהתאם לצורך, בין היתר, באמצעות קביעת תוכנית תרגולים אשר :
- 18.4.1. תגדיר את נושאי התרגול ויעדיו, את המתודולוגיה הנבחרת לתרגול, תדירותו, אופן הדיווח על תוצאות התרגול, תהליך זיהוי הפערים ביחס לתוכנית המשכיות העסקית הקיימת ועדכוניה בהתאם.
- 18.4.2. תכלול תרגולים עיוניים אסטרטגיים ותרגולים מעשיים שיבוצעו במטרה לבחון את אופן התאוששות מערכות המידע וההפעלה של תהליכים ושירותים חיוניים. כחלק מכך, התוכנית תכלול ביצוע תרגול עיוני ומעשי שמטרתו בחינת כשירות האתר החלופי, לכל הפחות, אחת לשנה.
- 18.4.3. תוכנית התרגולים כאמור תכלול, בין היתר, תרגולים שמטרתם בחינת הפעלת תוכנית ההיערכות לניהול אירועי אבטחת מידע כאמור בהוראה 301 בנושא ניהול המידע והגנתו.



- 18.5. **הכרזה על מצב חירום** - מינוי גורם בכיר שיהא האחראי להכרזה על מצב חירום וכן על הפעלת תוכנית המשכיות העסקית.
- 18.6. **מיגון אתרי הלשכה** - התייחסות לאופן מיגון האתר הראשי והחלופי של הלשכה לצורך צמצום נזקים פוטנציאליים בקרות אירוע אסון ובהתאם לצרכיה, ובהתאם למפורט בפרק ח'.
- 18.7. **תכנון עסקי וניהול פרויקטים** - התייחסות לאופן שילוב שיקולי המשכיות עסקית במסגרת קבלת החלטות עסקיות רלוונטיות, ובפרט בעת תכנון וניהול פרויקטים חדשים, השקת שירותים חדשים ופיתוח או רכישה של מערכות מידע.
- 18.8. **נותני שירות במיקור חוץ לתהליכים ושירותים חיוניים** - פירוט אופן ההתנהלות הנדרש מול נותני שירות במיקור חוץ לתהליכים ושירותים חיוניים, בין השאר, בהתאם למפורט בפרק ו'.

פרק ה' - תוכנית המשכיות עסקית

19. הלשכה תגבש תוכנית המשכיות עסקית (להלן - "התוכנית") שמטרתה להבטיח את יכולת הלשכה לפעול באופן רציף ולמזער את הפגיעה במתן שירותיה במקרה של הפרעה חמורה לעסקיה, ולאושש את פעילותה במקרה של אסון.
20. התוכנית תכלול הנחיות פעולה לתגובה מידית במקרה של שיבוש תפעולי משמעותי, בתרחישי הייחוס השונים הרלוונטיים עבור כלל התהליכים והשירותים החיוניים, וכן תביא בחשבון גם את הצעדים הנדרשים בטווח הארוך להחזרת מלוא הפעילות לשגרה.
- התוכנית תכלול, בין היתר, התייחסות למרכיבים הבאים:
- 20.1. **המשאב האנושי** - בהתבסס על ניתוח ההשלכות העסקיות, יוגדרו תחומי האחריות והסמכות של הצוות לניהול משבר, גורמי ההנהלה, צוותי עבודה, נותני שירות פנימיים וחינוניים, וגורמים אחרים. כמו כן, ימופו אנשי מפתח התומכים בתהליכים ובשירותים החיוניים, גורמים מגבים עבורם (לרבות גורמים מגבים עבור חברי צוות ניהול משבר), והנחיות להאצלת סמכויות במקרה של שיבוש תפעולי משמעותי המנטרל אנשי מפתח.
- 20.2. **תשתיות ומשאבים** - הלשכה תזהה ותמפה את התשתיות המשמשות אותה לתפקודה השוטף, כגון תשתיות פיזיות (מבנים, ציוד וכו'), תשתיות IT (תקשורת, שרתים, מערכות מידע לרבות כל מרכיבי הטכנולוגיה הנדרשים לשמירת הרציפות העסקית או לאישוש הפעילות, ממשקים לגורמים חיצוניים, תשתיות אבטחת מידע וכו') וכל תשתית אחרת. לאחר מכן, הלשכה תעריך את המשאבים והתשתיות הדרושים לה לקיום תהליכי עבודה חיוניים במצב חירום, ותבחן שימוש בחלופות אפשריות לצורך כך.
- 20.3. **תקשורת והסברה** - הלשכה תגדיר ממשקי תקשורת אשר יאפשרו קשר רציף וסדיר עם גורמים שונים (כגון: לקוחות, משתמשים בנתוני אשראי, ספקים, עובדים, רשויות פיקוח), לרבות ממשקי תקשורת להפצת מידע הן בקרב גורמים אלה והן בקרב הציבור הרחב, על מנת שידעו כיצד ליצור קשר עם הלשכה גם במקרה שערוצי התקשורת הרגילים יושבתו.
- 20.4. **ניהול משברים** - הלשכה תגדיר את תחומי האחריות של הצוות לניהול המשבר ושל בעלי התפקידים החברים בו, בהקשר ליישום התוכנית בלשכה, ואת אופן התנהלותה מול גופים חיצוניים כגון: גורמי רגולציה, משרדי ממשלה וארגוני חירום.



20.5. **אירועי אבטחת מידע** - הלשכה תקבע תוכנית היערכות להתמודדות עם אירועי אבטחת מידע בהתאם לעקרונות הקבועים בהוראה זו, וכן בהתאם להנחיות המפורטות בהוראה 301 בנושא ניהול המידע והגנתו.

20.6. **גיבוי נתונים** -

20.6.1. הלשכה תגדיר את אופן גיבוי הנתונים ומערכות המידע הרלוונטיים לתהליכים ושירותים חיוניים.

20.6.2. הלשכה תגדיר את אופן סנכרון הנתונים (replication) בין האתר הראשי לבין האתר החלופי ואת אופן הגיבוי בעותק נוסף על מנת להבטיח התאוששות גם במקרים בהם נפגע המידע באתר הראשי ובאתר החלופי שלה בו זמנית.

נהלי הגיבויים, כאמור בהוראה 301 בנושא ניהול המידע והגנתו, יתייחסו, בין היתר, לאופן יישום דרישות אלו.

20.7. **תוכנית התאוששות מאסון (Disaster Recovery Plan) / תוכנית התאוששות ממצב חירום** - הלשכה תגדיר תוכנית היערכות לשיקום מערכות המידע החיוניות לפעילותה, ככל שנפגעו בעת שיבוש תפעולי משמעותי. התוכנית תכלול הנחיות פעולה שיתיייחסו, בין היתר, לנושאים הבאים :

20.7.1. הפעולות הנדרשות לצורך מעבר לאתר החלופי וכן את הפעולות הנדרשות לחזרה ממנו. בכלל זאת, הלשכה תגבש מדריך טכני (Runbook) הכולל הנחיות מקיפות לגבי העלאת מערכות המידע מהאתר החלופי בהתאם ליעדי גיבוי הנתונים ויעדי ההתאוששות שהוגדרו, וכן החזרת המערכות לפעילות מהאתר הראשי בעת החזרה לשגרה. המדריך הטכני ומסמכים חיוניים נוספים יישמרו באתר החלופי גם בעותק קשיח, כגיבוי למקרה שלא תתאפשר גישה לקבצים האלקטרוניים.

20.7.2. גישה מרחוק במצב חירום לתשתיות המשמשות את הלשכה לתפקוד שוטף, כגון תשתיות פיזיות ותשתיות IT (לרבות מערכות מידע וממשקים לגורמים חיצוניים), הן של עובדים והן של נותני שירות, תוך זיהוי הסיכונים הכרוכים בגישה מרחוק וקיום מנגנוני בקרה ואבטחת מידע מתאימים.

20.7.3. אופן ההתאוששות מקבצי גיבוי (העותק הנוסף), ככל שהאתר הראשי והחלופי נפגעו בו זמנית.

20.7.4. חלופות למקרים בהם לא ניתן לבצע פעולות מהותיות באופן ממוחשב (לרבות שימוש בתהליכים ידניים), על מנת לעמוד ביעדי התאוששות, בקרות מפצות ואופן הזנת המידע למערכות המידע עם סיום מצב החירום.

20.8. **נותני שירות במיקור חוץ לתהליכים ושירותים חיוניים** - צעדים מתאימים על מנת לטפל בתוצאות הפוטנציאליות של הפרעה לעסקים עקב פגיעה ביכולת אספקת השירותים על ידי נותני שירות במיקור חוץ לתהליכים ושירותים חיוניים, ולחלופות לביצוע הפעילויות שהועברו למיקור חוץ כגון: החלפת נותן השירות או העברת הפעילות ללשכה (בהתאם למפורט בפרק ו').

20.9. **שינויים במצב חירום** - יש לקבוע כי שינויים שבוצעו במהלך שיבוש תפעולי משמעותי, יבוצעו על ידי גורמים מורשים ובאופן מפורקח ויתועדו כהלכה. שינויי חירום המנוהלים בצורה לקויה עלולים לגרום לשיבוש תפעולי נוסף.



21. עם סיום השיבוש התפעולי המשמעותי, על ההנהלה להכין תקציר מנהלים המשווה בין יעדים לתוצאות, חריגות מהותיות מהתוכנית, בעיות שזוהו והפקת לקחים, לרבות תוכניות פעולה לפתרון הבעיות עם תאריכי יעד.

פרק ו' - המשכיות עסקית של נותני שירות במיקור חוץ לתהליכים ושירותים חיוניים

22. הלשכה תפעל להפחתת הסיכונים הנובעים מתלות בנותני שירות במיקור חוץ לתהליכים ושירותים חיוניים (להלן - "נותן שירות"), זאת, בין השאר, בהתאם למפורט להלן וכן בהתאם למפורט בהוראה 301 בנושא ניהול המידע והגנתו לגבי מיקור חוץ או כל הוראה אחרת של הממונה בנושא מיקור חוץ.
23. הלשכה תעריך את יכולת נותן השירות לקיים רציפות עסקית כך שתימשך אספקת השירותים הרלוונטית ללשכה בתרחשי הייחוס השונים וכן תכלול במסגרת תוכנית התרגולים, כאמור בסעיף 18.4, בחינת הממשקים עם נותן השירות.
24. הסכם ההתקשרות עם נותן השירות יכלול את חובתו של נותן השירות להעמיד ללשכה שירותים גם בזמן חירום. הלשכה תוודא כי רמות השירות המוגדרות בהסכם תואמות את תוכנית המשכיות העסקית של הלשכה. הסכם ההתקשרות יכלול גם התייחסות לאחריות נותן השירות לקיים תוכנית המשכיות עסקית. בנוסף, בהתאם להערכתה את יכולת נותן השירות לקיים רציפות עסקית כאמור בסעיף 23, הלשכה תכלול בהסכם ההתקשרות עם נותן השירות, התייחסות לנושאים המפורטים להלן:
- 24.1. זכות הלשכה לקבל את תוכנית המשכיות העסקית הרלוונטית של נותן השירות;
- 24.2. זכות הלשכה לקיים ביקורת תקופתית על תוכנית המשכיות העסקית של נותן השירות, או לחילופין לקבל דוח ביקורת כאמור מגורם מבקר אחר שיהיה מקובל על הלשכה;
- 24.3. זכות הלשכה להשתתף בתרגילי ניהול המשכיות עסקית של נותן השירות או לקבל את ממצאי התרגול או לחילופין הסדרת השתתפות נותן השירות בתרגילי המשכיות עסקית שתבצע הלשכה מעת לעת.
25. על אף האמור לעיל, הלשכה אינה נדרשת לכלול בהסכם ההתקשרות עם נותן שירות שהוא ספק תשתיות לאומיות את הנושאים הקבועים בסעיף 24.

פרק ז' - אתר חלופי

26. על הלשכה לוודא את קיומו של אתר חלופי.
27. בעת קביעת האתר החלופי, הלשכה תתייחס, בין היתר, לפרמטרים הבאים: מיקום האתר כמפורט בסעיף 28, רמת המיגון כמפורט בפרק ח', גודל האתר, קיבולת העבודה בו והשירותים אשר נדרש לספקם בהתאם ליעדי התאוששות שנקבעו, תוך התייחסות למשך השיבוש התפעולי (טווח קצר, בינוני וארוך).
28. הלשכה תמקם את האתר החלופי כך שתקטן ההסתברות שהאתר החלופי והאתר הראשי יושפעו באופן דומה מתרחיש מסוים בעת שיבוש תפעולי משמעותי, ובכלל זה השפעה על מרכיבי התשתית הפיזית (חשמל, תקשורת וכדומה) המשמשים את האתרים. לצורך כך, יובאו בחשבון כלל תרחישי הייחוס. במטרה להקטין את ההסתברות ששני האתרים ייפגעו מאותו תרחיש, לרבות אפשרות של חסימת דרכי גישה, הלשכה תוודא, לכל הפחות, שהאתר החלופי יהיה ממוקם מחוץ למרחב העירוני של האתר הראשי של הלשכה.



29. היקף הציוד והמידע שיוחזק באתר החלופי ייקבע באופן שיבטיח את המשך פעילותה העסקית של הלשכה, במקרה שהאתר הראשי ייפגע באופן חמור.
30. האתר החלופי יהיה זמין באופן מידי לעבודה 24/7 לצורך עמידה ביעדי ההתאוששות שהוגדרו על ידי הלשכה, וייקבעו לגביו תקני איוש כוח אדם הנדרשים על מנת להבטיח את עמידות הלשכה בעת שיבוש תפעולי משמעותי.
31. היה ומפעיל האתר החלופי הינו נותן שירות במיקור חוץ, הלשכה תוודא כי לאותו נותן שירות יש את כל היכולות לשמור על תחזוקת האתר ומוכנותו לשעת חירום, וכן תפעל בהתאם למפורט בפרק ו'. הלשכה תבקר באופן תקופתי באתר החלופי על מנת לבחון את תחזוקת האתר ומוכנותו.

פרק ח' – יתירות ומיגון אתרים קריטיים

32. עבור כל אתר קריטי המשמש לעיבוד נתונים, הלשכה תוודא קיומם של שני קווי תקשורת לכל הפחות וכן יתירות ברכיבים חיוניים כגון אספקת החשמל, תשתיות הולכת החשמל ומערכות הקירור.
33. הלשכה תפעל למגן את אתריה הקריטיים על מנת לשמר המשכיות ורציפות במתן תהליכים ושירותים חיוניים בהתאם לסטנדרטים מקצועיים מקובלים.
- להלן עקרונות מנחים למיגון מינימלי של האתרים הקריטיים:
- 33.1. כל אתר קריטי ימוגן בפני מלחמה קונבנציונאלית;
- 33.2. אתר ראשי או חלופי, לפחות אחד משניים, יהיה עמיד בפני רעידת אדמה. במקרה בו האתר הראשי אינו עמיד בפני רעידת אדמה, הלשכה תחזיק בתוכנית אופרטיבית להעמדת שירותים חיוניים באתר החלופי בהתאם ליעדי התאוששות שנקבעו במסמך המדיניות;
- 33.3. בעת הקמת או מעבר לאתר קריטי חדש המשמש לעיבוד נתונים, יש לוודא כי לאתר מיגון מתאים לכלל תרחישי הייחוס וכי רמת ה-Tier לא תפחת מדרישות Tier3 בהתאם לסטנדרטים שנקבעו בתקן UpTime Institute (UTI) או תקן מקובל אחר, וזאת באמצעות קבלת אסמכתאות, למשל, תעודה מ-UTI או חוות דעת חיצונית מגורם מומחה בלתי תלוי.

פרק ט' - ביקורת פנימית

34. תכנית העבודה הרב שנתית של הביקורת הפנימית תכלול את בחינת מסגרת העבודה לניהול סיכוני המשכיות עסקית של הלשכה ואופן יישומה, בהתאם להוראה זו.
- הביקורת הפנימית תבחן, בין היתר, את תוכנית התרגולים של הלשכה בנושא ניהול המשכיות עסקית לצורך הערכת האפקטיביות של תוכנית המשכיות העסקית של הלשכה, לרבות בחינת ביצוע התרגולים בפועל, קיום תהליך הפקת לקחים וטיפול בממצאי התרגולים.



פרק י' - ביטוח

35. כיסוי ביטוחי הולם אינו מהווה תחליף לתכנית המשכיות עסקית אפקטיבית, אך יש בו לסייע בצמצום ההפסדים והנזקים כתוצאה משיבושים תפעוליים משמעותיים.
בהתאם, על ההנהלה לבצע סקירה שנתית לפוליסות הביטוח בכדי לבחון האם הכיסוי הביטוחי הקיים התבסס על תהליכי ניתוח ההשלכות העסקיות והערכת הסיכונים ובהתחשב בפרופיל הסיכון שלה.

פרק יא' – תחילה והוראות מעבר

36. תחילתה של הוראה זו שישה חודשים מיום פרסומה באתר מערכת נתוני אשראי בבנק ישראל (להלן- "יום התחילה").

37. על אף האמור בסעיף 36 :

37.1. תחילתו של סעיף 24 לעניין הסכמי התקשרות עם נותני שירות במיקור חוץ לתהליכים ושירותים חיוניים שנכרתו לפני מועד פרסום ההוראה, במועד חידוש ההסכם או בתום 12 חודשים מיום התחילה, המוקדם מביניהם.

37.2. תחילתם של סעיפים 28 ו-33 בתום 24 חודשים מיום התחילה, אולם הממונה רשאי להורות על דחיית מועד התחילה של סעיפים אלו לתקופה נוספת, ככל שיעלה הצורך.

* * *