

## ניהול סיכונים

### מבוא

1. מטרת הוראה זו לקבוע עקרונות להסדרת חובת הלשכה למסד מערך ניהול סיכונים אשר יוטמע בכל התהליכים בחברה, כחלק אינטגרלי מהם, במטרה להפחית את רמת הסיכון לה חשופה החברה, למנוע או לצמצם את התממשותם.
2. ההוראה קובעת עקרונות לניהול כלל הסיכונים שהדירקטוריון והנהלת הלשכה סבורים כי הלשכה חשופה להם, בכללם: סיכון תפעולי, סיכון מודל, סיכון הגנת המידע, סיכון ציות, סיכון מיקור חוץ, סיכון אסטרטגי וסיכון תדמית.
3. מערך ניהול הסיכונים בלשכה יכלול פעולות לזיהוי והערכת הסיכונים, מדידת החשיפות להם, נקיטת צעדי בקרה, פעולות להפחתת החשיפות וכן דיווח להנהלה ולדירקטוריון.
4. בקרות פנימיות המגולמות במהלך העסקים השגרתי של הלשכה יתוכננו כך שתבטחנה כי הלשכה מציינת למדיניות ניהול הסיכונים שלה וכן לחוקים ולתקנות החלים עליה.

### תחולה

5. ההוראה תחול על לשכת אשראי (להלן **הלשכה**) כהגדרתה בחוק נתוני אשראי, התשע"ו - 2016.
6. הממונה על שיתוף נתוני אשראי (להלן - **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 ונימוקיה אשר נמסרו לו בכתב, ורשאי הממונה לקבוע כי הפטור או ההוראות השונות יחולו לתקופה קצובה כפי שתיקבע על ידו.

### הדירקטוריון

7. הדירקטוריון אחראי לקיומה של תרבות ניהול סיכונים איכותית בלשכה. לצורך כך הדירקטוריון יאשר תכנית הדרכה בנושא ויעודד גיבוש של נורמות ותמריצים לעידוד התנהגות מקצועית ואחראית שתמנע חשיפה של הלשכה לסיכונים מיותרים.
8. הדירקטוריון יתווה את מדיניות ניהול הסיכונים בלשכה, יפקח על אופן ניהולם ויוודא כי הם מנוהלים באופן אפקטיבי.
9. לפחות אחת לשנה הדירקטוריון יקיים, דיון בנושאים הבאים:
  - 9.1. מדיניות ניהול הסיכונים - הדירקטוריון ייבחן ויאשר את נאותות מדיניות ניהול הסיכונים לרבות קיומן של הנחיות ברורות בנוגע למבנה הסמכויות והאחריות בלשכה ובכלל זה אחריות דיווחית, וכן יאשר שינויים במדיניות.
  - 9.2. סקר הסיכונים - הדירקטוריון ידון בתוצאות הסקר בהשלכותיו ובעדכונים שנעשו בו, בין היתר, על מנת לוודא כי סביבות הפיקוח והבקרה תואמות את מדיניות ניהול הסיכונים וכי מכלול הסיכונים מנוהלים בצורה אפקטיבית.
  - 9.3. הערכת הביקורת הפנימית - הדירקטוריון יודא שמדיניות ניהול הסיכונים של הלשכה כפופה לסקירה אפקטיבית ובלתי תלויה של פונקציית הביקורת הפנימית. בנוסף, יקיים הדירקטוריון

דיון יחד עם המבקר הפנימי, באשר להתרשמותו מרמת המודעות לסיכונים ומרמת הבקרה, תוך ציון מוקדי סיכון עיקריים.

10. דיווח תקופתי - הדירקטוריון יגדיר את מבנה הדיווח התקופתי שיאפשר לו מעקב אחר אופן ניהול החשיפות לסיכוני הלשכה, לרבות הגדרת הנושאים שיש לדווח אליו באופן מידי, ובכלל זה אירועים משמעותיים של התממשות סיכון וכמעט התממשות.

11. אישור שירות חדש - הדירקטוריון יאשר שירות חדש, לאחר שוודא מול כל הגורמים המקצועיים הרלבנטיים כי קיימים בידיהם משאבים ותשתיות נאותים וכי הם מיישמים תהליכי ניהול סיכון הולמים להפעלת השירות.

12. ביטוח - הדירקטוריון ידון ויאשר את רמת כיסוי הביטוח הנדרשת ללשכה, לרבות בהתאם לכללי נתוני אשראי (רישוי לשכות), התשע"ז-2017.

### ההנהלה

13. ההנהלה תפעל ליישום ולהטמעת מדיניות ניהול סיכונים אפקטיבית בהתאם להנחיות הדירקטוריון, ובכלל זה:

13.1. גיבוש ועדכון שוטפים של מסמכי המדיניות והנהלים לניהול סיכונים.

13.2. ביצוע סקר סיכונים תקופתי ועדכונ.

13.3. קיום דיון תקופתי בנוגע לסיכונים להם חשופה הלשכה ובתכנית ההפחתה לטיפול בסיכונים.

13.4. נקיטת פעולות מידיות לטיפול בהפרות משמעותיות ביחס למדיניות ניהול הסיכונים, לרבות שינוי, צמצום ואף הפסקת פעילות או שירות.

14. ההנהלה תדווח לדירקטוריון בהתאם לדרישות הדיווח שיגדיר ולכל הפחות כדלקמן:

14.1. דיווח מידי - על אירועים משמעותיים של התממשות סיכון או כמעט התממשות, לרבות ניתוח האירועים והבנת המשמעויות הנגזרות מהם.

14.2. דיווח תקופתי - על אופן ניהול הסיכונים בלשכה בצורה שתסייע לדירקטוריון להעריך את מידת האפקטיביות בה מנהלת הלשכה את הסיכונים להם היא חשופה.

15. ההנהלה תזהה ותעריך את הסיכונים הטמונים בהפעלת שירות חדש, טרם הפעלתו.

16. ההנהלה תוודא שפעילויות הלשכה מבוצעות על ידי עובדים בעלי ניסיון מתאים, יכולות טכניות וגישה למשאבים הדרושים.

### מדיניות ניהול הסיכונים

17. מדיניות הלשכה בנוגע לניהול הסיכונים תעוגן במסמך מדיניות שיכלול, לכל הפחות, את הנושאים הבאים:

17.1. הגדרה מלאה של כל הסיכונים להם חשופה הלשכה על מנת להבטיח השגת מטרות ניהול הסיכון, בכלל זה: סיכון תפעולי, סיכון מודל, סיכון הגנת המידע (לרבות סיכון פגיעה בפרטיות), סיכון ציות, סיכון מיקור חוץ, סיכון אסטרטגי וסיכון תדמית.

17.2. תיאור מערך התפקידים בלשכה ובכלל זה האחראיות הדיווחית.

17.3. קביעת מגבלות החשיפה לסיכונים השונים, ואופן הטיפול בהפרות.

17.4. תיאור תהליכי ניהול הסיכונים וסביבת הבקרה הפנימית המבטיחים ניהול נאות של הסיכונים להם חשופה הלשכה והפחתתם.

18. מסמך המדיניות ייסקר מעת לעת ויעודכן בהתאם להתפתחויות ולשינויים בסביבת הפעילות החיצונית והפנימית להן חשופה הלשכה.

### סקר סיכונים

19. המטרות בביצוע סקר הסיכונים הינן לזהות את כלל הסיכונים להם חשופה הלשכה, להעריך את משמעותיות החשיפה לסיכונים שזוהו ולתת המלצות לניהול החשיפה לסיכונים והפחתתם.

20. סקר הסיכונים יבוצע לפחות אחת לשנה ויעודכן באופן שוטף בהתאם לצורך.

21. הסקר יכסה את כל התהליכים העסקיים מקצה לקצה (כולל, בין השאר, תשתיות, מערכות מידע וכוח אדם) ויכלול התייחסות פרטנית לסיכונים המהותיים להם חשופה הלשכה בכל תהליך, בקרות קיימות והמלצות לצמצום הסיכון.

22. בעת ביצוע סקר הסיכונים תיעזר הלשכה, בין היתר, בניתוח אירועי התממשות סיכונים או אירועים של כמעט התממשות וכן בממצאי דוחות ביקורת של המבקר הפנימי או הממונה.

### שירות חדש

23. הלשכה תקבע מדיניות לאישור שירות חדש אשר תסדיר את תהליכי הבדיקות והאישור הנדרשים טרם הפעלתו. מדיניות כאמור תובא לאישור הדירקטוריון.

24. מסמך המדיניות יכלול הגדרה של שירות חדש. לעניין זה, "שירות חדש" יכלול מלבד פעילות או שירות חדשים גם שינויים משמעותיים או הרחבה משמעותית של פעילות או שירות קיימים.

25. תהליך אישור שירות חדש יתבצע על ידי כל הגורמים המקצועיים הרלבנטיים ובכלל זה: יעוץ משפטי, ניהול סיכונים, מנהל טכנולוגיית המידע, ממונה אבטחת מידע, הנהלה ודירקטוריון, ויכלול לכל הפחות:

25.1. הערכה של הסיכונים הגלומים בשירות החדש.

25.2. בחינה של הכלים והמומחיות הנדרשים על מנת לזהות, להעריך, לבקר, לצמצם ולדווח על הסיכונים הגלומים בשירות החדש.

26. בשנה הראשונה להפעלת השירות החדש, יתקיים תהליך להערכת הסיכונים ורמת הביצועים של השירות שאושר, ביחס להערכות המוקדמות שנעשו בעת אישור השירות, ויבוצעו התאמות בתהליכי ניהול הסיכונים במידת העניין.

### דיווחים לממונה

27. הלשכה תדווח לממונה על:

27.1. אירוע בו התממשו סיכונים אשר כתוצאה מהם נפגעה משמעותית יכולת הלשכה לספק שירותים ללקוחותיה, או נפגעה יכולת הלשכה לעמוד בהוראות הממונה או הוראות כל דין, או נפגע משמעותית אמון הציבור בלשכה. הדיווח יועבר לממונה תוך 3 שעות ממועד הזיהוי הראשוני של האירוע.

27.2. אירוע של כמעט התממשות סיכונים שהיה עלול להביא לפגיעה משמעותית בלקוחות או באמון הציבור בלשכה. הדיווח יועבר לממונה תוך 7 ימים ממועד הזיהוי הראשוני של האירוע.

28. הלשכה תדווח לממונה על תוצאות התחקיר שבוצע לאירוע, כאמור בסעיף 27, ועל לקחים ופעולות שבוצעו בעקבותיו ככל שנדרש. דיווח ראשוני יועבר לממונה תוך 3 ימים ודיווח נוסף תוך 30 ימים מהמועד שהאירוע הסתיים.

29. הלשכה תדווח לממונה על מדיניות ניהול הסיכונים אחת לשנה ולא יאוחר מ-30 ימים מתום השנה הקלנדרית.

30. הלשכה תדווח לממונה מראש על שינויים מהותיים במדיניות ניהול הסיכונים ולא יאוחר מ-30 ימים טרם ביצוע השינוי.

31. הלשכה תדווח לממונה מראש על כוונתה להפעיל שירות חדש ולא יאוחר מ-60 ימים טרם הפעלתו.

32. הלשכה תעביר לממונה את סקר הסיכונים לא יאוחר מ-14 ימים ממועד ביצועו ואת התכנית להפחתת הסיכונים לא יאוחר מעשרה ימים מהמועד האמור.

\* \* \*