[לוגו החברה]	**רשימת תיוג אבטחת מידע בארגון**	מהדורה: _____
	מספר טופס:_____	בתוקף מתאריך:_____

מבצע/י הסקר	תפקיד	תאריך	מצב העבודה בחברה בשלב ביצוע הסקר

נושא נסקר	הבקרה	מצב	ציין פרטים
ניהול נכסים וסיכונים	נכסי מערכות מידע בכלל ומאגרי מידע בפרט מנוטרים ומבוקרי?		
	קיים הליך סיווג מידע		
	קיים הליך השמדת מצעי מידע המכילים מידע רגיש		
	הוגדר הליך ניהול סיכונים תקופתי		
קריפטוגרפיה / הצפנה	במידה ויש שימוש במידע רגיש במיוחד, האם הוגדרה שיטת הגנה והצפנה		
אבטחה פיזית וסביבתית	הכניסה למתחם החברה מבוקרת ומנוטרת - ציין הגנות ובקרות		
	קיים מידור למקומות רגישים, ציין את המקומות		
	הגישה למקומות ממודרים לעובדים מורשים בלבד. האם רשימת המורשים מאושרת?		
אבטחת התפעול	קיימים נהלים והנחיות לניהול מערכות המידע		
	קיימות הגנות ובקרות כנגד תכנות זדוניות וגישה לא חוקית (FW AV) פרט		
	הוגדר תהליך שיחזור ובקרה מתבצע שיחזור מדגמי		
	קיימת מערכת אשר מנטרת את פעילות מערכות המחשב בכלל וההגנות בפרט		
	קיימת התראה בעת חשש לפגיעה במערכת		
אבטחת תקשורת	קיים תרשים רשת מפורט אשר מציג את מערכות הארגון והבקרות הקיימות		
	הוגדר תהליך מאובטח של העברת / קבלת מידע רגיל ורגיש מהארגון ומחוצה לו, ולהיפך.		
	קיים הסכם על העברה / קבלת מידע בין הארגון לגורם חיצוני		
פיתוח	הוגדר תהליך פיתוח הכולל הבטי אבטחת מידע		

[לוגו החברה]	**רשימת תיוג אבטחת מידע בארגון**	מהדורה: _____
	מספר טופס:_____	בתוקף מתאריך:_____

נושא נסקר	הבקרה	מצב	ציין פרטים
יחסים עם ספק	הוגדר תהליך בקרת ספקים בהיבטי אבטחת מידע		
	ספקי הארגון חתומים על הסכם סודיות		
ניהול אירוע אבטחת מידע	הוגדר תהליך דיווח ותחקור אירועי אבטחת מידע, הכולל הפקת לקחים		
	מתקיים תחקור והפקת לקחים עם קרות אירוע אבטחת מידע		
הגנה על הארגון - עבודה מרחוק	העובד קיבל הנחיות אבטחת מידע לעבודה מרחוק		
	העובד מודע שאין לשמור כל מידע ארגוני בכלל ורגיש בפרט במחשב האישי.		
	קיימת רשימת משתמשים מורשים מאושרת לעבודה מרחוק ע"י נציג הנהלה		
	הגישה לרשת הארגונית מרחוק, דרך רשתות ציבוריות ואחרות, מתבצעת בטווח מוגן HTTPS, תוך שימוש בפרוטוקול הצפנה מוכר SSL VPN כדוגמא		
	קיימת מדיניות סיסמאות מוקשחת (8 תווים מורכבים, 3 ניסיונות עד נעילה, היסטוריה סיסמא 10 דורות)		
	הגישה מרחוק לרשת הארגונית מחייבת הזדהות כפולה 2FA		
	במחשב של המשתמש העובד מרחוק מותקנות הגנות ובקרות עדכניות FW AV של הארגון		
	מתבצעת נעילת מסך תוך 10 דקות של אי שימוש במחשב (שומר מסך עם סיסמא)		
	קיים גיבוי אוטומטי לרשת הארגונית		
	קיימת הצפנת הדיסק הפנימי כאשר יש צורך בשמירת מידע ארגוני בכלל ורגיש בפרט במחשב נייד / אישי.		
	קיימת מערכת ניטור בארגון אשר מתעדת כל גישת משתמשים לרשת הארגונית מרחוק.		
	קיימת מערכת ניטור לבחינת שימוש לא נאות ע"י משתמשים מרחוק (אנומליות, שעות לא סבירות, הורדת קבצים גדולים)		

[לוגו החברה]	**רשימת תיוג אבטחת מידע בארגון**	מהדורה: _____
	מספר טופס:_____	בתוקף מתאריך:_____

נושא נסקר	הבקרה	מצב	ציין פרטים
	הארגון משתמש מערכת DLP למניעת דלף מידע Data Loss Prevention Software		
	הנהלת הארגון מודעת לסיכונים בעבודה מרחוק באמצעות מחשב נייד או המחשב האישי של המשתמש מהבית		
	המשתמש מכיר תהליך דיווח במקרה של חשד לאירוע אבטחת מידע בעת העבודה מרחוק / מהבית		
היבטי אבטחת מידע של ניהול המשכיות העסקית	הוגדרה תכנית להתנהגות בעת אירוע חריג / אסון והדרך להמשך פעילות ומתן שירות ללקוח		
	זוהו תהליכים חיוניים לפעילות בעת חירום (מגפה / מלחמה / אי יכולת לעבוד במתחם החברה)		
	לעובדים חיוניים יש יכולת לעבודה מחוץ למתחם החברה		
	התוכנית להמשכיות עסקית כוללת הבטי אבטחת מידע		
תאימות	זוהו התקנים והחוקים בהיבטי אבטחת מידע שהארגון מחויב להם		
	הארגון משתמש בתוכנות חוקיות בלבד		
	הארגון עומד בדרישות תקנות הגנת הפרטיות		
	הארגון מקיים מבדקי אבטחת טכניים במערכות המידע שלו (חוסן, PT)		

סיכונים אפשריים ודרכים למזעורם:

זיהוי הסיכון	השלכות אפשריות	חומרה 1-5	הסתברות 1-5	עוצמת סיכון 1-5	פעולות לניהול	
					פעולה	אחראי

* עוצמת הסיכון= חומרה X הסתברות. כשרמת הסיכון 12-25 יש חובה לקבוע פעולה מיידית לניהול הסיכון ולייישמה.

כשרמת הסיכון 6-12 יש לקבוע פעולה לניהול הסיכון עד 3 חודשים מיום השלמת רשימת התיוג וליישמה לפי לוח הזמנים שנקבע.

לשאלות נוספות והתייעצויות - אנחנו כאן ***Nadav@nasecurity.co.il // milo@mixum.co.il***