התחייבות לשמירה על סודיות, אבטחת מידע

עיריית בית שמש

כללי:

הוראות נספח זה חלות על ספקים אשר במסגרת עבודתם נדרשים לשהות באזורי המזמין ו/או לקבל זכות גישה (פיזית או לוגית) למערכות המידע ותשתיות המחשוב.

הוראות נספח זה באות להוסיף על הוראות ההסכם ולא לגרוע מהן. מובהר כי דרישות אבטחת המידע והסייבר של הרשות המפורטות בנספח זה, הינן בנוסף לדרישות אבטחת המידע שהוגדרו על ידי מערך הסייבר או המשכ"ל (ככל שההתקשרות הינה מכוח מכרז מרכזי שלהם), ואינן גורעות מהן.

מובהר כי העבודה והעיבוד יתבצעו אך ורק על גבי תשתיות המזמין או תשתיות ענן הנמצאות בשליטתו המלאה (On-Premise, ענן מנוהל, או סביבות עבודה שיתופיות) וללא שמירת מידע אצל הספק. עמידה בהוראות אלו הינה תנאי סף לביצוע העבודה.

הגדרות:

"מידע": מידע עסקי, מסחרי או טכנולוגי המצוי במאגרי המזמין או שהספק נחשף אליו במסגרת עבודתו. הגדרה זו כוללת גם "מידע אגבי": מידע שהגיע לידיעת הספק באקראי (שמיעת שיחות, צפייה במסכים/מסמכים, זהות מבקרים).

"מידע אישי": נתון הנוגע לאדם מזוהה או לאדם הניתן לזיהוי, "אדם הניתן לזיהוי" - מי שניתן לזהותו במאמץ סביר, במישרין או עקיפין, ובכלל זה באמצעות פרט מזהה, כגון שם, מספר זהות, מזהה ביומטרי, נתוני מיקום, מזהה מקוון או נתון אחד או יותר הנוגע למצבו הפיזי, הבריאותי, הכלכלי, החברתי או התרבותי.

"מידע בעל רגישות מיוחדת":

מידע על צנעת חיי המשפחה של אדם, על צנעת אישיותו ועל נטייתו המינית.

מידע המתייחס למצב בריאותו של אדם, ובכלל זה מידע רפואי לפי חוק זכויות החולה.

מידע גנטי, כהגדרתו בחוק מידע גנטי.

מזהה ביומטרי המשמש או מיועד לשמש לזיהוי אדם או לאימות זהותו באופן ממוחשב.

מידע על מוצאו של אדם.

מידע על עברו הפלילי של אדם.

מידע על דעותיו הפוליטיות של אדם או אמונותיו הדתיות או השקפת עולמו.

"סביבה מאובטחת / תשתיות המזמין": כל סביבת מחשוב המצויה בשליטת המזמין, לרבות:

מערכות פנים-ארגוניות (On-Premise).

חיבור מרחוק באמצעות VPN, RDP, 365.

מערכות ענן וסביבות שיתופיות המנוהלות על ידי המזמין בהן למזמין יש שליטה מלאה על הרשאות הגישה והמידע.

"עובדי הספק": לרבות עובדים, קבלני משנה, יועצים, מתכנתים וכל גורם הפועל מטעם הספק לצורך ביצוע ההסכם.

<u>אבטחה פיזית, בקרת כניסה והתנהלות ברשות:</u>

אבטחה פיזית: הספק מאשר כי ידוע לו שהכניסה לאזורי המזמין כפופה לנהלי הביטחון של הרשות ולמערך האבטחה הקיים (לרבות שומרים, מצלמות, בקרת כניסה וכו'). עובדי הספק ישתפו פעולה באופן מלא עם גורמי הביטחון.

ליווי ותנועה: תנועת עובדי הספק תעשה אך ורק בליווי נציג המזמין בלבד. למעט אזורים שהוגדרו ואושרו על ידי אגף מערכות מידע, חדשנות וטכנולוגיה כאזורים "ללא ליווי" לביצוע העבודה.

איסור סיוע לעקיפת נהלים: חל איסור מוחלט על עובד הספק להכניס אדם נוסף לרשות או לפתוח דלתות עבור גורמים שאינם מורשים (גם אם הם עובדים מוכרים), אלא באישור מפורש.

דיווח על אובדן: במקרה של אובדן תג כניסה, מפתח פיזי, או רכיב הזדהות דיגיטלי (Token/כרטיס חכם), ידווח הספק למנהל מוקד מצלמות המזמין באופן מיידי מרגע הגילוי.

<u>שמירה על סודיות ומניעת חשיפה:</u>

הספק מתחייב לשמור בסודיות גמורה כל מידע שנחשף בפני עובדיו, בין אם מתוך מערכות המידע ובין אם באופן אגבי (שיחות מסדרון/טלפון/מראה עיניים וכד').

מניעת חשיפה ברשתות חברתיות: הספק ועובדיו מתחייבים שלא לתעד, לצלם, להקליט או לפרסם כל פרט הנוגע למתרחש באזורי המזמין. איסור זה כולל הפצה בעל-פה או בכתב (לרבות רשתות חברתיות) של מידע אודות התנהלות פנים-ארגונית, שיחות מסדרון, מידע על נבחרי ציבור או בכירים ששהו במקום או כל אירוע חריג אחר אליו נחשפו.

חובת הסודיות הינה ללא הגבלת זמן ותחול גם לאחר סיום ההתקשרות.

<u>אבטחת גישה לוגית, ציוד קצה ועבודה מרחוק (בחצרות המזמין):</u>

כפיפות לנהלי הרשות: עם קבלת הרשאת גישה למערכות, יחולו על עובד הספק מלוא נהלי אבטחת המידע של המזמין (לרבות נהלי פיתוח מאובטח לספקים המפתחים בחצרות המזמין), ועליו לפנות באופן יזום למנהל מטעם המזמין לקבלתם ולהטמעתם. בנוסף, העובד ישתלב במערך המודעות הארגוני (בהתאם לרמת החשיפה והנחיות ממונה אבטחת המידע), לרבות ביצוע לומדות, מעבר הדרכות והשתתפות בסימולציות Phishing הנערכות על ידי המזמין, כתנאי להמשך הגישה.

תקינות ציוד קצה: במידה והגישה תתבצע באמצעות ציוד מחשוב של הספק (מחשב נייד/נייח חיצוני), הספק מתחייב כי הציוד יעמוד בדרישות האבטחה של המזמין. המזמין רשאי לבצע בדיקת תקינות ("Sanity Check") לציוד כתנאי לחיבור.

עבודה בסביבה מבודדת ומניעת זליגת מידע (DLP): העבודה תתבצע אך ורק בתוך "סביבת העבודה" שהוגדרה (החלון המרוחק, הדפדפן המאובטח או ממשק הענן). חל איסור מוחלט לבצע העתקה של קבצים, נתונים או מידע מתוך סביבת המזמין אל המחשב המקומי של הספק. איסור זה כולל שימוש בפונקציות "העתק-הדבק" החוצה, צילומי מסך לשמירה מקומית, הורדת קבצים מסביבת המזמין למחשב האישי, או יצוא קבצים לתיבות דואר פרטיות.

איסור אגירת מידע: חל איסור מוחלט על הספק לנהל מאגרי מידע של המזמין אצלו. כל המידע יישמר אך ורק על תשתיות המזמין (לרבות בענן המנוהל על המזמין).

איסור שימוש בכלי בינה מלאכותית (AI): חל איסור מוחלט להזין ו/או להעלות מידע עסקי ארגוני, קוד מקור או מידע אישי ו/או מידע בעל רגישות מיוחדת לכלי AI פתוחים. שימוש בכלי AI יותר אך ורק באישור מראש ובכתב מממונה אבטחת המידע.

<u>הגנת הפרטיות, ניהול זהויות וניטור:</u>

הגנת הפרטיות: הספק מתחייב לפעול בהתאם להוראות חוק הגנת הפרטיות ותקנותיו.

עקרון "הצורך לדעת": הגישה למידע תיעשה אך ורק בהיקף המינימלי הנדרש לביצוע המשימה. חל איסור מוחלט על עובדי הספק לשוטט במערכות, לבצע שאילתות על מכרים, שכנים או בני משפחה, או לגשת למידע שאינו רלוונטי במישרין לעבודתם.

ניהול משתמשים: הגישה תינתן באמצעות שם משתמש אישי בלבד. חל איסור מוחלט על שימוש בסיסמאות משותפות או העברת פרטי הזדהות.

הסכמה לניטור: הספק מצהיר כי הוא ועובדיו מודעים לכך שכל הפעולות המבוצעות בתשתיות המזמין (לרבות תעבורת רשת, דואר אלקטרוני, קבצים, גישה למאגרים ופעילות בענן) מתועדות ומנוטרות באופן שוטף ע"י מערכות האבטחה.

<u>מהימנות עובדים:</u>

בדיקות רקע ע"י הספק: הספק מתחייב שלא להעסיק עובדים בעלי עבר פלילי רלוונטי (עבירות מחשב, מרמה, פרטיות).

<u>סיום העסקה וביטול הרשאות:</u>

חובת דיווח מיידית: הספק מתחייב להודיע למזמין באופן מיידי וללא דיחוי (ולכל המאוחר תוך 24 שעות) על כל מקרה של סיום העסקת עובד בעל הרשאות גישה, או על כל הפסקת עבודה זמנית ממושכת (כגון: חל"ת, חופשת לידה, מילואים ממושכים, השעיה או חופשה העולה על 30 יום), וזאת לצורך הקפאה או חסימה של הרשאות הגישה לאלתר.

חובת דיווח על שינוי תפקיד: כמו כן, ידווח הספק מיידית על כל שינוי בתפקיד העובד הגורע את הצורך בגישה למערכות המזמין או לחלקן.

חובת דיווח מיוחדת בגין עבירות משמעת וטוהר מידות: על אף האמור בסעיף לעיל, במקרה בו סיום ההעסקה (או השעיית העובד) נובע מנסיבות של חשד לעבירת משמעת, אי-סדרים, עבירה פלילית, מעילה באמון, גניבה, הונאה או עבירת מחשב, מתחייב הספק לדווח על כך באופן ישיר, מיידי ודיסקרטי למנהל מוקד מצלמות המזמין או לממונה אבטחת המידע (בנוסף לדיווח התפעולי). הדיווח יכלול את פרטי החשד או האירוע, וזאת על מנת לאפשר למזמין לבצע בחינה של פעולות העובד במערכות, ניטור לאחור (Forensics), שלילת דליפת מידע ובקרת נזקים.

<u>אחריות והצהרה:</u>

הספק מתחייב להחתים כל עובד מטעמו, בטרם כניסתו לחצרי המזמין, על כתב התחייבות אישי לשמירת סודיות וביטחון בנוסח המצורף כנספח א' לנספח זה.

הטפסים החתומים יישמרו במשרדי הספק וישלחו למנהל מוקד מצלמות המשרד/ממונה אבטחת המידע כתנאי לתחילת העסקה.

<u>חתימת הספק :</u>

אני הח"מ מצהיר כי קראתי את נספח אבטחת המידע, הבנתי את תוכנו, ואני מתחייב לפעול על פיו ולהנחות את עובדיי בהתאם.

שם הספק: _____ ח.פ: _____ שם החותם: _____

חתימה וחותמת: _____ תאריך: _____

נספח א': כתב התחייבות עובד/קבלן משנה - גישה למערכות, מידע ואזורים

אני הח"מ: _____ ת"ז: _____

עובד בחברת: _____ (להלן "הספק") מועמד לעסוק בתפקיד: _____

מבקש לקבל הרשאת כניסה לאזורי הארגון ו/או גישה למערכות המידע שלו (להלן: "הרשות"), ומתחייב בזאת באופן בלתי חוזר כדלקמן:

1. **הגדרות והבנת מהות המידע: הובהר לי כי במסגרת עבודתי אני עשוי להיחשף למידע רגיש ביותר, לרבות "מידע אישי" ו/או "מידע בעל רגישות מיוחדת" כהגדרתו בחוק הגנת הפרטיות ועליי לציית להוראות ותקנות הגנת הפרטיות לרבות שמירת סודיות מוחלטת. כמו כן, ידוע לי כי חובת הסודיות חלה גם על "מידע אגבי" - דברים שראיתי או שמעתי במקרה (שיחות מסדרון, מסכים של אחרים, זהות מבקרים ברשות וכד').**

שמירת סודיות ופרטיות: אני מתחייב לשמור בסודיות מוחלטת כל מידע שאליו איחשף. לא אעתיק, לא אצלם, לא אדפיס ולא אעביר מידע זה לשום גורם (לרבות בני משפחה, חברים או עמיתים לעבודה שאינם מוסמכים). אני מתחייב לגשת אך ורק למידע שחיוני לביצוע המשימה שלי. חל איסור מוחלט לבצע שאילתות או לחפש מידע על מכרים, שכנים, בני משפחה או אישיות ציבורית מתוך סקרנות.

אבטחת מידע וסייבר: אני מתחייב לעבוד אך ורק בתוך סביבת העבודה שהוקצתה לי (RDP, VPN, מחשב משרדי או ענן מנוהל). חל איסור מוחלט לשמור קבצים של הרשות על המחשב האישי שלי (או על הלפטופ של הספק). חל איסור מוחלט לשלוח חומרים מהעבודה לתיבת המייל הפרטית שלי (Gmail/Walla וכו') או לשירותי ענן חיצוניים (Google Drive/Dropbox פרטיים). לא אבצע צילומי מסך (Screenshots) ולא אשתמש אעתיק או אשתמש במניפולציות דומות כדי להוציא מידע החוצה. במידה ואני מתחבר מרחוק, אני מצהיר כי המחשב שלי מוגן (מערכת הפעלה חוקית ומעודכנת, אנטי-וירוס פעיל), ואין בו תוכנות פיראטיות או תוכנות שיתוף קבצים. הסיסמה שנמסרה לי היא אישית. לא אעביר אותה לאף אדם (גם לא למנהליי) ולא אאפשר לאף אדם לעבוד על היוזר שלי. אני מתחייב שלא להשתמש בכלי בינה מלאכותית לצורך ביצוע עבודתי. ידוע לי כי חל איסור מוחלט להזין, להעתיק או לטעון לכלי AI כלשהו קוד תוכנה, מסמכים פנימיים, נתונים אישיים או לבצע שאילתות מזהות על מידע רשותי. אני מצהיר כי ידוע לי שאני כפוף לנהלי אבטחת המידע הארגוניים, ועלי לפנות לממונה עליי לקבלתם. כמו כן, אני מתחייב לשתף פעולה עם מערך המודעות של הרשות, לרבות: ביצוע לומדות, מעבר מבחני ידע, והשתתפות בתרגילי פישינג ככל שיידרש ממני.

ביטחון פיזי ונוהלי התנהגות ברשות: אני מתחייב להישמע להוראות אנשי הביטחון. אני מתחייב שלא לפתוח דלתות עבור אנשים אחרים ולא לאפשר לאף אדם להיכנס אחריי ללא העברת תג, גם אם הם נראים כעובדים

מוכרים, אלא אם קיבלתי אישור מפורש. לא איכנס לאזורים שלא הוגדרו לי, ובמידת הצורך אמתין לליווי או לאישור מנהל מוקד מצלמות.

מניעת חשיפה: חל איסור מוחלט לצלם, להקליט או לתעד כל דבר בתוך אזורי המשרד (בטלפון נייד או בכל אמצעי אחר). אני מתחייב שלא לפרסם שום פרט על המתרחש ברשות ברשתות חברתיות או שיתוף חוויות על דברים שראיתי או שמעתי במסגרת שהותי (ויכוחים, אירועים, אישים שביקרו).

הסכמה לניטור: אני מצהיר כי הובא לידיעתי שכל הפעולות שאבצע במערכות המחשוב שהוקצו לי ע"י הרשות (כולל גלישה באינטרנט, תכתובות מייל, גישה לקבצים) ובאזורי הרשות, מנוטרות, נרשמות ונשמרות לצרכי אבטחת מידע. אני נותן בזאת את הסכמתי המלאה לביצוע ניטור זה ומוותר על כל טענה לפגיעה בפרטיות בהקשר זה.

חובת דיווח וסיום עבודה: אני מתחייב לדווח מיידית למוקד התמיכה או למנהל מוקד מצלמות על: אובדן תג/סיסמה, חשד לאירוע אבטחה, או אם הבחנתי באדם חשוד. עם סיום עבודתי או יציאה לחופשה ממושכת, אדווח על כך ואחזיר כל אמצעי גישה שנמסר לי.

סנקציות והצהרה משפטית: ידוע לי כי הפרת התחייבות זו עלולה להוות עבירה על חוק הגנת הפרטיות, התשמ"א-1981 ותקנותיו, ועל חוק העונשין, ועלולה לחשוף אותי לתביעות אזרחיות, הליכים פליליים והרחקה לצמיתות ממתן שירותים לרשות.

ולראיה באתי על החתום:

שם פרטי ומשפחה: _____ חתימה: _____ תאריך: _____