מועצה אזורית הגלבוע

נוהל A.15.1.1 – מדיניות אבטחת מידע עבור יחסים עם ספקים

על פי תקן ישראלי ISO/IEC 27001:2013

מהדורות מסמך:

מס״ד	תאריך	עודכן ע״י	תיאור השינוי
1	30.7.2019	עזרא דיין	גרסה ראשונה

בקרת מסמך:

גורם	פרטי גורם	תפקיד	תאריך	חתימה
עורך	עזרא דיין	יועץ		
בודק	רונן בגים	מנמ״ר		
מאשרת	ענת מור	מנכ״לית		

1. כללי

1.1. המועצה אזורית הגלבוע (להלן: ״**המועצה**״) מקבלת שירותים שונים ומגוונים מספקים חיצוניים הפועלים הן בממד הפיסי והן בממד הקיברנטי.

1.2. רוב השירותים המסופקים מטעם הספקים החיצוניים מצריכים נגישות ברמות ובתצורות שונות אל סביבת העבודה השוטפת של המועצה.

1.3. שירותים המסופקים בממד הפיסי מצריכים נגישות פיסית אל שטח המועצה הכולל את המבנים השונים, לרבות משרדי העובדים.

1.4. שירותים המסופקים בממד הקיברנטי מצריכים נגישות אל מערך המחשוב של המועצה, הכולל מידע רגיש, לרבות פרטים אישיים של תושבי מועצה אזורית הגלבוע ונתונים עסקיים ציבוריים.

1.5. לאור נגישותם של גורמים חיצוניים, סביבת העבודה השוטפת של המועצה חשופה לאירועי אבטחת מידע, בממד הפיסי והקיברנטי, אשר עלולים להיגרם כתוצאה מהתממשות איומים מסוגים שונים ולהוביל לפגיעה בתפקוד המועצה על ידי השחתה ו/או חשיפה של מידע רגיש.

1.6. אי לכך, עולה הצורך הבלתי מתפשר למזער ככל הניתן את הסיכוי הממשי להתרחשותם של אירועי אבטחת מידע, ובכך גם את הסיכוי להתממשותה של פגיעה בפעילות המועצה ולקוחותיה.

1.7. נוהל זה יפרט את הנחיות אבטחת המידע הנדרשות למימוש כמסגרת ההתקשרות והעבודה עם ספקים חיצוניים, הן בממד הפיסי והן בממד הקיברנטי.

2. מטרות

2.1. לפרט את תהליכי העבודה הנדרשים לביצוע על ידי בעלי התפקידים המפורטים בנוהל זה, בעת עבודתם מול ספקים של המועצה בתחומי אבטחת מידע.

2.2. הנוהל מיועד לעובדי המועצה, לקבלן המחשוב של המועצה (להלן: "הקבלן"), ספקי מערכות המחשוב וספקים נוספים בתחומי מערכות המידע של המועצה, משתמשי המועצה וכל גורם המחזיק במידע השייך למועצה. הנוהל מחייב כל גורם המטפל בשרתים במועצה ו/או בתחנות העבודה ו/או במאגרי המידע של המועצה.

3. הגדרות

3.1. **מידע**: כל נתון הנוגע ו/או הקשור לפעילותו, תפעולו או תפקודו של המועצה, לרבות מידע הנוגע לצנעת הפרט ומידע רגיש, הקיים על-גבי אמצעי אחסון ממוחשבים, מגנטיים או אלקטרונים, על-גבי מצעי מידע פיזיים וכן המועבר בעל-פה.

3.2. **אבטחת מידע**: מכלול הפעולות והאמצעים הננקטים והמיושמים במועצה, שמטרתם להביא לכך שהמידע ופריטי הציוד היוצרים אותו ומטפלים בו, יוגנו מפני פגיעה, חשיפה או שינוי, במזיד או בשוגג, הן מתוך המועצה והן מחוצה לו.

3.3. **מנהל אבטחת מידע**: מנהל האחראי על אבטחת המידע במועצה, אשר מנחה ונותן תמיכה בתחום אבטחת המידע במועצה ואשר מנחיל את החלטות וסיכומי ועדת היגוי לאבטחת המידע.

3.4. **ספק**: ספק חיצוני של מערכות מחשוב, תקשורת, מערכות מידע, מערכות בקרה וכל מערכת אחרת הנכללת בתחום מדיניות אבטחת המידע, עליו חלה החובה ליישם את דרישות אבטחת המידע ולהשתתף בתרגול ובקרות על פי מדיניות אבטחת המידע של המועצה והרגולציה החלה עליה.

3.5. **אורח**: גורם שאינו נמנה על עובדי המועצה, אשר קיבל היתר מוגבל בזמנים לשהות במתחמי העבודה של המועצה ו/או לגשת ולעשות שימוש במידע פומבי המפורסם על ידי המועצה כדוגמת אתר אינטרנט, תכתובות דואר, העברת קבצים, שרטוטים ותוכנית וכיו״ב.

3.6. **שימוש אסור**: פעולה המבוצעת מבלי לקבל היתר לביצועה על-פי נהלי המועצה ו/או פעולה שהותרה לביצוע, אך אינה ״כשרה״ בנסיבות ביצועה.

3.7. **אירוע סייבר**: מקרה בו עובד או מערכת ניטור הקיימת ברשות המועצה או ברשות ספקי המחשוב ומערכות המידע, מעריכים עפ״י המידע העומד לרשותם ו/או על פי תסמינים כגון השתלטות על מחשב המועצה, פעילות לא סבירה (אנומליה, תהליכים שאינם מוסברים) של שרת או מערכת מידע תפעולית או ארגונית, כי קיימת או עלולה להתקיים מתקפה על מערכות המחשוב של המועצה ו/או על מאגרי המידע ו/או על נכסים דיגיטליים של המועצה.

3.8. **מערך המחשוב**: כלל התשתיות והמערכות הממוחשבות המשמשות את בעלי התפקידים במועצה לטובת פעילותיה לרבות ציוד ממוכן, תשתיות טכנולוגיות, שרתים, מחשבים נייחים וניידים, ציוד תקשורת וכו׳.

4. מסמכים ישימים

4.1. תקן ת״י ISO 27001:2013 – פרק A.15.1.1, פרק A.15.1.2

5. שיטה – מדיניות אבטחת מידע עבור יחסים עם ספקים

5.1. מסגרת כללית

5.1.1. המועצה מפעילה ספקים לטובת פעילות כגון ניהול, עיבוד, אחסון או פיתוח של המידע שברשותה על ידי גורמי צד שלישי בשיטת מיקור חוץ.

5.1.2. המועצה מקבלת שירותים באמצעות כוח אדם חיצוני המופעל על ידי ספקים חיצוניים שאינם עובדי המועצה.

5.1.3. עם זאת, אין בכך בכדי לגרוע מאחריותה של המועצה לוודא את קיום נהלי אבטחת המידע ברמה הנדרשת ובאופן הנדרש, כפי שמוגדרים במדיניות אבטחת המידע, גם במקרים בהם השירות ניתן בפועל על ידי ספקים חיצוניים.

5.1.4. מדיניות אבטחת המידע, הכוללת שמירה על סודיות, שלמות המידע ואמינותו, זמינות המידע ושרידותו - תיושם גם במסגרת פעילות המבוצעת עבור המועצה על ידי גורמי צד שלישי ו/או במסגרת קבלת שירותים מספקים חיצוניים, בדגש על ההנחיות המפורטות בנוהל זה.

5.1.5. כל התקשרות עם ספק חיצוני בין אם באופן ישיר או במסגרת מכרז, לטובת קבלת שירות ו/או רכש אמצעים מכל סוג (לרבות אמצעים טכנולוגיים), תבוצע בכפוף לעקרונות וההנחיות המפורטים כנוהל זה.

5.2. שיטת עבודה

5.2.1. התקשרות מול ספק חיצוני תבוצע בהתבסס על הגדרה פרטנית של תחומי הפעילות הנדרשים למימוש השירות מטעם הספק; סוג השירות, לוחות הזמנים, אזורי הפעילות, רמת הנגישות וזהות הגורמים המבצעים.

5.2.2. במסגרת התהליך יבוצע מיפוי של האיומים הפוטנציאליים אשר עשויים להתממש במסגרת ההתקשרות, במטרה להגדיר את פעולות התגובה הנדרשות לביצוע במקרים של חריגה מנהלי אבטחת המידע.

5.2.3. הסכם ההתקשרות מול הספק החיצוני יכלול התייחסות בכתב לדרישות הנוגעות למימוש נהלי אבטחת המידע, לרבות חובת השמירה על נהלי אבטחת המידע וההסכמה לפיקוח מצד המועצה ו/או ממוני ביקורת מטעמה.

5.2.4. באחריותה של המועצה לוודא כי ספק השירותים החיצוניים שומר על עקרונות אבטחת מידע נאותים על מנת להגן על נכסי המידע מפני דליפה, שינוי או מחיקה.

5.2.5. אי לכך, נדרשת המועצה להגדיר קריטריונים מקדמיים שיוודאו את יכולת הספק החיצוני לעמוד בדרישות למימוש נהלי אבטחת המידע.

5.2.6. במהלך תקופת ההתקשרות יבוצעו ביקורות שוטפות של הספק החיצוני, על ידי המועצה או ממונים מטעמה, במטרה לוודא את מימוש נהלי אבטחת המידע.

5.3. אבטחת המידע - בקרות פיסיות

5.3.1. הרשאות לגורם חיצוני יוענקו באופן אישי, מוגבל בזמן ובהתאם לצורך בלבד.

5.3.2. תהליך מתן ההרשאות יבוצע על ידי מנהל אבטחת המידע או נציג מוסמך מטעמו ויתועד לשם בקרה ופיקוח.

5.3.3. לא יוענקו הרשאות גישה לאזורים שאינם רלוונטיים לשירות המסופק, בדגש על אזורים המוגדרים בעלי רמת רגישות גבוהה.

5.3.4. גישתם של גורמים חיצוניים תבוצע בתיאום מראש ובפיקוח מנהל אבטחת המידע או נציג מוסמך מטעמו (מומלץ להסמיך בעל תפקיד מקצועי בתחום הפעילות של הספק).

5.3.5. לא יוענקו אמצעי הזדהות קבועים לגורמים חיצוניים על מנת שלא תתאפשר נגישות עצמאית.

5.3.6. זמני כניסה ויציאה של גורמים חיצוניים יתועדו באמצעות רישום (ידני ו/או ממוחשב) לטובת פיקוח ובקרה.

5.3.7. ככל שניתן, תתקיים הפרדה בין אזורי הפעילות השוטפת של עובדי המועצה ובין אזורי מתן ו/או קבלת שירותים חיצוניים.

5.3.8. במקרים בהם לא ניתן לבצע הפרדה בין הסביבות, ילווה הגורם החיצוני על ידי מנהל אבטחת המידע או נציג מוסמך מטעמו.

5.3.9. בכל מקרה יחול איסור על ספקים חיצוניים לנוע בסביבת המשרדים של עובדי המועצה ללא תיאום ופיקוח.

5.3.10. אזורים אליהם מורשים לגשת ספקים חיצוניים לא יכילו מידע המסווג כרגיש (בדגש על פרטים אישיים של תושבים וצרכנים).

5.3.11. ספקים חיצוניים שידרשו לגשת אל אזורים המוגדרים בעלי רמת רגישות גבוהה, ילוו על ידי מנהל אבטחת המידע או נציג מוסמך מטעמו הבקיא בתחום העיסוק הרלוונטי לאזור הרגיש.

5.3.12. נדרש לוודא כי הפעילות המבוצעת על ידי הגורמים החיצוניים תואמת את סוג השירות הנדרש מאותו ספק.

5.3.13. חל איסור להעביר אל ספקים חיצוניים מידע מכל סוג, בדגש על מידע רגיש, שאיננו רלוונטי לתחום עיסוקם.

5.3.14. במקרים בהם עולה צורך רלוונטי להעביר מידע רגיש אל ספק חיצוני, יש לבחון את הסיכונים הכרוכים בתהליך ולצמצם ככל שניתן את הפוטנציאל להתממשות אירוע דליפת מידע.

5.3.15. נדרש להחיל איסור על ספקים חיצוניים לעשות שימוש באמצעי צילום ו/או הקלטה בסביבת המשרדים ו/או באזורים מאובטחים המוגדרים בעלי רמת רגישות גבוהה.

5.3.16. נדרש להחיל איסור על ספקים חיצוניים לחבר אמצעי מדיה נתיקה אל סביבת המחשוב של המועצה. בכלל זה, מכשירים סלולאריים, אמצעי מדיה נתיקה (DOK) וכו׳.

5.3.17. נדרש להחיל איסור על ספקים חיצוניים לקבל ו/או להעתיק ו/או לצלם מסמכים המכילים מידע שאינו רלוונטי לתחום עיסוקם, בדגש על מידע רגיש.

5.3.18. נדרש להחיל איסור על ספקים חיצוניים לשהות באזורים שאינם רלוונטיים לפעילותם ו/או שאינם מורשים לגשת אליהם, בדגש על אזורים המוגדרים בעלי רמת רגישות גבוהה.

5.3.19. באחריות ספק חיצוני שברשותו מסמכים שאינם רלוונטיים לתחום השירות שמספק, להחזירם לאלתר בתצורת המקור (ללא עותקים) אל המועצה.

5.4. אבטחת המידע – בקרות לוגיות

5.4.1. הרשאות גישה לספק חיצוני אל מערך המחשוב של המועצה יוענקו באופן אישי, בהתאם לשירות המסופק ועל פי עקרונות המידור.

5.4.2. התחברות ספקים חיצוניים אל מערך המחשוב תחייב לכל הפחות הזדהות באמצעות שם משתמש וסיסמה חזקה.

5.4.3. יודגש בפני הספק החיצוני כי נתוני ההזדהות אל מערך המחשוב של המועצה הנם אישיים ולא ניתנים להעברה.

5.4.4. לא יוענקו הרשאות גישה לסביבות שאינן רלוונטיות לשירות המסופק, בדגש על אזורים המוגדרים בעלי רמת רגישות גבוהה.

5.4.5. ייקבע פרק זמן של אי פעילות (Session Time Out) במערכת שלאחריו יופעל מנגנון ניתוק תקשורת שיחייב הזדהות מחדש. במידה ומנגנון הניתוק מטיל מגבלה על פעילות בעלת אופי רציף, יש להתריע לפני ניתוק התקשורת.

5.4.6. לא תבוצע התקנה ו/או הסרת התקנה של תוכנות מכל סוג במערך המחשוב ללא תיאום פרטני וקבלת אישור פוזיטיבי מטעם אחראי אבטחת המידע במועצה.

5.4.7. גישה מרחוק למערך המחשוב של המועצה תבוצע אך ורק בתיאום מראש עם אחראי אבטחת המידע, לאחר קבלת אישור פוזיטיבי להתחברות ובהתאם להרשאות.

5.4.8. גישה מרחוק תבוצע מסביבה מאובטחת, באמצעות אמצעי קצה עליהם מותקנים רכיבי הגנה בסיסיים לפחות ובתווך מוצפן בלבד.

5.4.9. הפעולות שיבוצעו על ידי הספק החיצוני (לרבות התחברות והתנתקות) יתועדו לשם פיקוח ובקרה של אחראי אבטחת המידע במועצה, באמצעות כלי ההגנה והניטור המוטמעים במערך המחשוב.

5.5. אבטחת מידע - בקרת רשומות

5.5.1. פעולות הכרוכות בעיבוד, אחסון או העברה של מידע ו/או נגישות לתשתיות ו/או סביבת הניהול של מערך המחשוב - יחייבו אישור פרטני של אחראי אבטחת המידע במועצה.

5.5.2. ככל שניתן, תבוצע הפרדה בין הסביבות השונות במערך המחשוב, לטובת צמצום הנגישות של ספקים חיצוניים אל סביבות המכילות מידע רגיש.

5.5.3. יש להחיל איסור ו/או להגביל את האפשרות של ספקים חיצוניים המתחברים למערך המחשוב לגשת אל תחנות הקצה של עובדי המועצה.

5.5.4. יש להחיל איסור ו/או להגביל את האפשרות של ספקים חיצוניים המתחברים למערך המחשוב לעשות שימוש בתוכנות המאפשרות לצלם ו/או להקליט מרחוק.

5.5.5. יש להחיל איסור ו/או להגביל את האפשרות של ספקים חיצוניים המתחברים למערך המחשוב לגשת אל אזורים שאינם רלוונטיים לפעילותם ו/או שאינם מורשים לגשת אליהם, בדגש על אזורים המוגדרים בעלי רמת רגישות גבוהה.

5.5.6. יש להחיל איסור ו/או להגביל את האפשרות של ספקים חיצוניים המתחברים למערך המחשוב להוציא ו/או להעתיק קבצים מכל סוג ללא אישור פרטני.

5.5.7. אמצעי קצה המכילים מידע ומיועדים להשמדה או תחזוקה על ידי ספק חיצוני לא יכילו נתונים רגישים.

5.5.8. מדיית זיכרון שהכילה מידע רגיש תוצא לצורכי תחזוקה רק לאחר שננקטו אמצעים מספקים למחיקת המידע באופן המונע אפשרות שחזור המידע באמצעים טכנולוגיים.

6. תרגול ובקרות

6.1. על פי תוכנית עבודה שנתית ליישום תרגול ובקרות המפורטת בקובץ תוכנית עבודה ליישום, תרגול עובדים שנתית של המועצה אשר תאושר על ידי ממונה אבטחת המידע במועצה.

6.2. התוכנית תכלול לכל הפחות את הרכיבים הבאים:

6.2.1. הדרכה לספקים – בתחומי אבטחת מידע, ציות, מהימנות, כללי עשה ואל תעשה, מקרים ותגובות. ההדרכות יתקיימו לפחות פעמיים בשנה על פי תוכנית עבודה שנתית.

6.2.2. תרגולים – ביצוע תרגול – ערנות ספקים על פי תוכנית עבודה שנתית.

6.2.3. בקרות – בקרת קיום הדרכות שנתית.

7. אחריות

7.1. האחריות ליישום נוהל זה חלה על ספקי מערכות מידע ומחשוב של המועצה.

7.2. מנמ״ר המועצה ומי מטעמו אחראי לבקרת היישום של הדרישות.

8. נספחים

8.1. תוכנית תרגול ובקרות שנתית

8.2. נספח התחייבות ספק לשמירה ולעמידה בדרשות אבטחת מידע של המועצה.

נספח התחייבות ספק לאבטחת מידע

הואיל; ואנו החתומים מטה (להלן: **הספק**) נותנים למועצה אזורית הגלבוע (להלן: **״המועצה״**) שירותים, המתבססים על מידע של המועצה;

והואיל; ומתן השירותים למועצה מותנה בהתחייבות שלנו לשמור על הסודיות של המידע של המועצה ועל אבטחת מידע זה, כמפורט בכתב זה;

אי לכך, אנו מתחייבים בזאת כדלקמן;

א. הספק ימנה אחראי לאבטחת המידע. על אחראי אבטחת המידע להבטיח שימוש נכון בזיהוי המשתמש ובסיסמא, בהרשאות הגישה למידע ובהגנת משאבי מערכות המחשב והמידע ומערכות התקשורת. כמו כן ימנה הספק ממונה לאבטחה הפיזית של המידע ומערכות המידע והתקשורת.

ב. תהיה הגנה פיזית ובקרת גישה למחשבים, לשרתים ולרכיבי התקשורת כגון Routers, Switches.

ג. הגישה למערכות המחשוב המחזיקות מידע של המועצה, תתאפשר רק תוך שימוש בזיהוי (User-ID) אישי ובסיסמאות אישיות וחסויות. הסיסמאות תהיינה ידועות רק למשתמשים בלבד ותוחלפנה לפחות כל 6 חודשים.

ד. זיהוי משתמש יינעל אוטומטית לאחר 3 שגיאות רצופות בהקשת הסיסמא. השחרור יוכל להתבצע רק ע״י האדמיניסטרטור ומי שהוסמך למלא את מקומו בהיעדרו או על ידי קוד אימות זיהוי.

ה. תנוהל מערכת הרשאות למורשי גישה.

ו. תופעל מערכת ניהול הרשאות ויצירת רמות הרשאה המפרידות בין מנהלי הרשת לעובדים אחרים. חשבונות וזכויות של אדמיניסטרטור יינתנו למנהלי הרשת בלבד.

ז. ייושם מידור פנימי בשרת בגישה לספריות וקבצים של המועצה. הגישה לספריות וקבצים אלה תתאפשר רק למי שעבודתם ותפקידם מטעם הספק מחייבים זאת.

ח. תותקן תוכנת הגנה תקנית ומעודכנת כנגד וירוסים.

ט. לא יוצאו דיסקים משרתים או מדיות מגנטיות אחרות לתיקון או לכל מטרה אחרת כשעליהם נמצאים קבצים ונתונים של המועצה. במקרה כזה יש למחוק את המידע ולפרמט את הדיסק.

י. יוקם נוהל עבודה מסודר להעברת, אחסון ותחזוקת מדיה מגנטית, או אופטית עם מידע של המועצה כך שלא תועבר מדיה ללא תיאום מוקדם. הנוהל יוקם בשיתוף של נציג המועצה, מנהל מאגר המידע של המועצה וממונה על אבטחת מאגרי המידע המועצה.

יא. מדיה מגנטית או אופטית כנ״ל תאוחסן בתאום עם המועצה במקום שהגישה אליו תתאפשר למורשי גישה בלבד.

יב. בתחנות העבודה תשמר אבטחת המידע:

יג. לא יישמרו קבצים של המועצה על הדיסק הקשיח של התחנה.

יד. בכל תחנה יותקן נועל מסך עם סיסמא.

טו. הכניסה לרשת תהיה באמצעות USER ID אישי.

טז. המערכת תנעל משתמש לאחר 5 ניסיונות גישה כושלים. שחרור נעילה ייעשה רק על ידי המוקד הטכני של הספק ולאחר וידוא כי המשתמש הוא זה המזוהה מולם על ידי פרטי מידע נוספים (כגון ת.ז. ומספר טלפון נייד).

יז. לא ניתן יהיה להוריד קבצים של המועצה מהשרת באמצעות התחנה.

יח. גיבויים יבוצעו בצורה מסודרת וישמרו במקום סגור ונעול עם גישה לאחראי על הגיבויים בלבד. הגיבוי יבוצע על בסיס יומי ויכלול את כל נתוני המועצה. גיבוי מלא של כל נתוני המועצה יועברו על גבי מדיה מגנטית פעם בחודש לספק המחשוב של המועצה. מדיה אחת עם נתוני תוכנת המוקד ומדיה נוספת עם נתוני האפליקציה העירונית . באחריות הספק לבצע בדיקת שחזור נתונים כדי לוודא שתהליך הגיבוי תקין.

יט. אין להעביר קלטות עם גיבויים לגופים חיצוניים.

כ. כל מדיה מגנטית, או אופטית, או דוח השייכים למועצה או שהם תוצרי עיבוד מנתוני המועצה, יאוחסנו בארון סגור וכן יושמדו ויגרסו לאחר השימוש.

כא. אין להוציא חומר לגריסה או השמדה חיצונית ללא תאום עם המועצה.

כב. הספק מצהיר כי הוא פועל כנדרש על פי החוק, התקנות ותיקוני הגנת הפרטיות וכי הוא נוקטת באמצעי אבטחה ובקרה כמתחייב מהוראות חוק הגנת הפרטיות, תיקוניו ותקנותיו.

כג. הספק מתחייב להחתים את עובדיה על הצהרות סודיות, הכוללים, בין היתר, התחייבות לשמירה מוחלטת על סודיות המידע של המועצה.

כד. הספק מתחייב להודיע למנהל מחלקת המחשוב של המועצה על כל חשד לגניבה ו/או פריצה ו/או העתקה ו/או חדירה למסמכים שברשותי ו/או למדיה אלקטרונית ו/או שנמצאים בטיפולי ו/או כל ניסיון לעשות כך, באופן מיידי וללא שהות.

כה. בסיום פעילותי מול המועצה, אני מתחייב/ת למסור לגורם מולו אני פועל במועצה את כל המסמכים, המידע וכל חומר אחר שהגיע או הוכן על ידי במהלך העבודה.

כו. הספק מתחייב לאפשר לנציג המועצה לערוך ביקורת אבטחה בכל עת.

ולראייה באנו על החתום:

_____	_____	_____	_____
הספק	שם (משפחה ופרטי)	חתימת הספק	תאריך