

לכבוד:

אוניברסיטת אריאל בשומרון

תאריך: _____

הנדון: נספח אבטחת מידע עבור ספק השומר מידע של אוניברסיטת אריאל בשומרון

1. כללי

- 1.1. כחלק מפעילותה העסקית וכפועל יוצא מתהליכי עבודה, אוניברסיטת אריאל בשומרון (להלן: "האוניברסיטה"), אוספת, מנהלת, מחזיקה במידע ועשויה להעביר סוגי מידע שונים הנמצאים ברשותה, לספקים חיצוניים (להלן: "הספק") לצורך מתן שירות שוטפים.
- 1.2. מסמך זה כולל אוסף דרישות אבטחת מידע כלליות עבור ספקי האוניברסיטה, לצורך התקשרות עימה. ייתכן וחלק מהדרישות אינן רלוונטיות לספק כזה או אחר בהתאם לאופן השימוש במידע ומנגד ייתכנו הנחיות נוספות שיעברו לספק מעת לעת ובהתאם לצורך.
- 1.3. עמידה בהוראות מסמך זה הינה תנאי סף להתקשרות עם הספק ויהיו חלק בלתי נפרד מהסכם ההתקשרות עימו. על הספק לעמוד בדרישות אבטחת מידע אלו כחלק ממתן שירותיו לאוניברסיטה, כפי שיעודכנו מעת לעת.
- 1.4. האחריות ליישום הנחיות אבטחת המידע הינה על הספק. הוראות אבטחת המידע החלות על הספק יחולו גם על ספקי משנה וצדדים שלישיים עמם הספק חולק את המידע המועבר אליו.

2. הצהרת שימוש במידע

- 2.1. הספק מתחייב כי יעשה שימוש במידע המועבר אליו מהאוניברסיטה אך ורק למטרות לשמם הוא מועבר, בהתאם למפורט בהסכם עם החברה ובכפוף להצהרת הסודיות עימה הוא חתום.
- 2.2. הספק מתחייב שלא לגלות את המידע אלא לצורך מתן השירותים לאוניברסיטה ובכפוף להנחיותיה.
- 2.3. הספק מתחייב לעדכן את האוניברסיטה בכל אחד מהמקרים הבאים:
 - 2.3.1. שינוי בפרטי הספק

- 2.3.2. בכל בקשה ו/או פנייה, שהתקבלה אצל הספק מנשוא המידע ו/או מצד שלישי כלשהו, בנוגע למידע, לרבות בקשה לעיון ו/או תיקון המידע
- 2.3.3. בכל בקשה לגילוי המידע מרשות מוסמכת כלשהי או על פי צו בית משפט.

3. מינוי נאמן אבטחת מידע וסייבר

- 3.1. במסגרת הסכם ההתקשרות של הספק עם האוניברסיטה, יידרש הספק למנות נאמן אבטחת מידע מקרב עובדיו ו/או גורם אחר מטעמו, ויגדיר את סמכויותיו ותפקידו אשר יכללו, בין היתר, עמידה בדרישות נספח זה.
- 3.2. נאמן אבטחת המידע יהיה גורם אמון על כל מערך אבטחת המידע של הספק לרבות יישום דרישות אבטחת מידע אלו.
- 3.3. חובתו של נאמן אבטחת המידע לדווח על אירועי אבטחת מידע הרלוונטיים לאוניברסיטה, תוך 72 שעות מתחילת האירועים, לרבות אירועים של אובדן, גניבה או דליפה של מידע. בדיווחים יועברו פרטים אודות הפעולות שננקטו בעקבות גילוי האירועים וכל מידע שעלול להשפיע על האוניברסיטה ו/או עלול להסב לה נזק.
- 3.4. האוניברסיטה רשאית לדרוש את העברת קבצי ה-LOG ממערכות הספק לצורך בדיקה ותחקור.
- 3.5. הספק נדרש לדווח לאוניברסיטה ולנהל רשימת ספקי משנה אשר מועבר אליהם מידע ותומכים בשירותים הניתנים לה.

4. ביקורת אבטחת מידע

- 4.1. הספק מתחייב לאשר לאוניברסיטה או למי מטעמה לבקר באתר הספק או בכל אתר אחר בו נשמר המידע וזאת בכפוף להודעה מראש, של 14 יום לפחות.
- 4.2. הביקורת יכללו בקרות טכנולוגיות בתחום התשתיות והאפליקציה, בקרות על תהליכים ארגוניים וקיום נהלי עבודה, בקרות אבטחה פיזית, מבדקי חזירה וכל מבדק אחר שהאוניברסיטה תימצא לנכון.
- 4.3. זוח הליקויים יועבר על ידי האוניברסיטה לספק לצורך מתן התייחסות לליקויים ולטיפול בהם.
- 4.4. הספק יחויב לתקן את הליקויים בפרק הזמן אשר יוגדר בשיתוף עם האוניברסיטה.

4.5. לאחר סיום תיקון הליקויים, יודיע הספק לאוניברסיטה כי הליקויים תוקנו.

5. ניהול רשת

5.1. גורמי אבטחת המידע של האוניברסיטה רשאים לדרוש מהספק פירוט מלא של מערכות המחשוב שברשותו והמשמשות לביצוע עבודתו עבור האוניברסיטה.

5.2. במידת הצורך, גורמי אבטחת המידע של האוניברסיטה ימסרו לספק מפרטי הקשחה מעודכנים, אשר יחייבו את הספק לפעול על פיהם ולהודיע בכתב לאוניברסיטה על סיום פעולת ההקשחה במערכות המחשוב.

5.3. רשתות אלחוטיות

5.3.1. הספק יקיים הפרדה לוגית של הרשת הארגונית מרשת האינטרנט ומרשתות ציבוריות אחרות, באמצעות רכיב אבטחתי, דוגמת FW.

5.3.2. במידה וקיימת רשת אלחוטית, הרשת תאובטח על ידי תקני אבטחת מידע מקובלים ותכלול לכל הפחות סיסמת גישה לרשת. הרשת האלחוטית לא תאפשר גישה למידע של האוניברסיטה ו/או למערכות מידע אשר מאחסנות מידע של האוניברסיטה.

5.4. הפרדת סביבות

5.4.1. הספק יקיים הפרדה בין סביבות עבודה שונות בהן מאוחסן המידע של האוניברסיטה, כדוגמת: סביבות פיתוח, בדיקות, ייצור וכדומה.

5.4.2. הספק יקפיד כי לא יאוחסן מידע של האוניברסיטה בסביבות הנמוכות. ככל שנשמר מידע של האוניברסיטה בסביבות אלו, יש להטמיע אמצעי הגנה וביצוע ניהול הרשאות זהים לסביבת הייצור.

6. אבטחת תחנות קצה ושרתים

6.1. מערכות ההפעלה המותקנות על גבי תחנות הקצה והשרתים של הספק יהיו עדכניות ונתמכות על ידי היצרן. הספק יבצע עדכוני מערכת הפעלה באופן תדיר.

6.2. על גבי תחנות הקצה והשרתים יותקנו אמצעי אבטחה מקובלים, אשר יכללו לכל הפחות, תוכנת אנטי וירוס עדכנית בעלת חתימות עדכניות.

- 6.3. על גבי תחנות הקצה והשרתים תוגדר נעילת מסך עם סיסמה לאחר אי פעילות, ולכל היותר לאחר פרק זמן של 15 דקות של אי פעילות.
- 6.4. ככל הניתן, הספק יטמיע מערכת לבקרת התקנים על מנת למנוע התפרצות של וירוסים ו/או נזקות בתחנות הקצה או בשרתים. במידה ולא מתאפשר הדבר, יגדיר הספק, לכל הפחות, סריקה של ההתקנים בעת חיבור לתחנות הקצה.

7. רכיבים ניידים לרבות מחשבים ניידים

- 7.1. מחשבים ניידים יכילו את כלל אמצעי ההגנה והאבטחה אשר מיושמים על תחנות הקצה של הספק, לפי ההנחיות בסעיף לעיל.
- 7.2. מחשבים ניידים המאחסנים מידע של האוניברסיטה יוצפנו על מנת למנוע גישה למידע בעת גניבה ו/או אובדן של המחשב הנייד.
- 7.3. הספק יגדיר נהלי שימוש ברכיבים ניידים (מדיה מגנטית, מדיה נתיקה, מחשבים ניידים, טלפונים ניידים וכדומה) שיכללו התייחסות להגנה פיזית והגנה לוגית של הרכיבים.
- 7.4. מדיה מגנטית / נתיקה
- 7.4.1. מדיה מגנטית ומדיה נתיקה המאחסנת מידע של האוניברסיטה תישמר באופן מאובטח ותסומן כמכילה מידע רגיש. כאשר לא מבוצע בה שימוש, המדיה תישמר במגירה ו/או ארון נעול.
- 7.4.2. בתום השימוש במדיה המגנטית או במדיה הנתיקה, הספק יימחק לחלוטין את המידע השמור על גבי המדיה באופן שלא יהיה ניתן לשחזרו.

8. בקרת גישה

- 8.1. ניהול משתמשים
- 8.1.1. הגישה לאמצעי המחשוב של הספק יתבססו, לכל הפחות, על שם משתמש וסיסמה.
- 8.1.2. לכל משתמש יוקצו אמצעי זיהוי אישיים וחד ערכיים אשר יזוהו עם העובד.
- 8.1.3. לא יאופשר שימוש במשתמשים גנריים, למעט שימוש במשתמשים לצורך הפעלת תהליך ממוכן (משתמשים אפליקטיביים).

8.2. ניהול הרשאות

- 8.2.1. לכל משתמש יוענקו הרשאות בהתאם לעיקרון הצורך לדעת ולבצע.
- 8.2.2. הספק יישם רמות הרשאות המפרידות והמגבילות את המשתמשים בביצוע פעולות בתחנות הקצה (כגון: ניתוק תוכנת האנטי וירוס) וזאת בהתאם לחלוקת תפקידים וסמכויות.

8.3. גישה מרחוק

- 8.3.1. הספק ינקוט באמצעי אבטחה נאותים בכל הקשור להתחברות מרחוק אל הרשת הארגונית שלו.

8.4. מדיניות סיסמאות

- 8.4.1. הספק יגדיר מדינות סיסמאות אשר עומדת בתקני אבטחת המידע המקובלים. מדיניות זו תיושם ברשת הארגונית ובמערכות המידע של הספק המכילות מידע של האוניברסיטה.
- 8.4.2. מדיניות הסיסמאות תכיל את הפרמטרים הבאים:
- 8.4.2.1. אורך סיסמה בעלת 8 תווים, לכל הפחות.
- 8.4.2.2. יישום של מורכבות סיסמה אשר תכלול מספרים, אותיות ותווים מיוחדים.
- 8.4.2.3. החלפת סיסמה אחת ל-90 יום.
- 8.4.2.4. שמירת היסטוריית סיסמאות עד 10 דורות אחרונות.
- 8.4.2.5. נעילת משתמש לאחר 5 ניסיונות גישה כושלים.

9. משאבי אנוש ומודעות עובדים

- 9.1. הספק יבצע בדיקות נאותות אשר מקובלות בתהליך מיין וגיוס עובדים וזאת בהתאם לרגישות המשרה ולמידע אליו נחשף במסגרת תפקידו.
- 9.2. מובהר בזאת כי האוניברסיטה תהיה רשאית, על פי שיקול דעתה הבלעדי לדרוש מעובדי הספק לבצע מבדקי מהימנות במידת הצורך. בכל מקרה שתוצאות הבדיקה כאמור לא תהינה לשביעות רצונה של האוניברסיטה, תהיה רשאית האוניברסיטה לדרוש מהספק למנוע מאותו עובד גישה למידע וכן להחליפו בגורם ו/או אדם אחר.

9.3. הספק יבצע הדרכות לעובדיו אודות נהלי אבטחת המידע ויחתים אותם על הצהרה לשמירת סודיות ושמירת על כללים נאותים בעת שימוש במידע של האוניברסיטה בהתאם להנחיות נספח זה.

9.4. בעת סיום העסקה של עובד, הספק יוודא כי כלל הרשאות הגישה שלו בוטלו, בפרט הרשאות למידע של האוניברסיטה.

10. אבטחה פיזית

10.1. כללי

10.1.1. הספק יישם אמצעי הגנה פיזיים נאותים במתחם המשרדים לרבות מנגנון בקרת כניסה למתחם, כגון: מערכת בקרת כניסה, קודן וכדומה.

10.1.2. אמצעי ההגנה הפיזיים יכללו מערכת אזעקה, מערכת מצלמות וכדומה.

10.1.3. הספק יגדיר נהלי אבטחה פיזית, על מנת לצמצם גישה של גורמים בלתי מורשים למתחם המשרדים, לרבות נהלי ליווי אורחים וגורמים זרים.

10.1.4. הספק יישם מדיניות לשמירה על מסמכים המכילים מידע של האוניברסיטה ("שולחן נקי") במתחם המשרדים.

10.1.5. ציוד פיזי המכיל מידע (שרתים, כוננים וכדומה) וארונות תקשורת ימוגנו במעגל אבטחה נוסף, כדוגמת: דלת תקינה עם נעילה, קודן, מערכת בקרת כניסה וכדומה.

10.1.6. ככל שהשירות אותו נותן הספק נדרש להיות זמין ומגובה באתר שלו, ייודא הספק כי יש ברשותו מערכות בטיחות ומניעת כשל תפעולי כדוגמת חיבור מערכת אל פסק (UPS), גלאי נפח, מערכות גילוי, התראה וכיבוי בעת שריפה (גלאי עשן, מתזי מים, רכזת התראה ואמצעים נוספים), רצפה צפה, גלאי הצפה וכדומה.

10.2. מסמכים וציוד

10.2.1. מסמכים או ציוד המכילים מידע של האוניברסיטה יישמרו בארונות נעולים ו/או במגירות נעולות בשעה שלא מבוצע בהם שימוש.

10.2.2. מסמכים או ציוד המכילים מידע של האוניברסיטה ייגרסו או ייגרטו במידה ואין בהם צורך.

11. סיום התקשרות עם הספק וביקורת מסכמות

11.1. עם סיום ההתקשרות של האוניברסיטה עם ספק ו/או סיום התקשרות של ספק עם ספקי

משנה וקבלני צד שלישי, יבוצעו הפעולות הבאות:

11.1.1. מחיקת כלל המידע הלוגי השמור במערכות המחשוב של הספק ובמצעים

דיגיטליים, בהתאם להוראות הדין ובהתאם לדרישות האוניברסיטה.

11.1.2. השמדת כלל המידע הפיזי השמור באתר הספק, הן גריסה והן גריטה של מצעים

פיזיים.

11.1.3. באחריות הספק להשמיד את כל המצעים הדיגיטליים אשר לא ניתן לבצע בהם

כתיבת-על או להעבירם לידי מחלקת אבטחת המידע של האוניברסיטה לצורך

השמדתם.

11.1.4. הספק יוודא כי לא יישארו אצלו עותקים של הנתונים והמידע אשר היה בשימוש

השייך לאוניברסיטה.

11.2. האוניברסיטה רשאית, בהתאם לשיקול דעתה, לבצע ביקורת מסכמת בכל אתרי הספק,

במטרה לוודא כי הפעולות המוזכרים לעיל בוצעו כנדרש ועל פי שביעות רצונה.

ולראייה באנו על החתום:

חתימה וחותמת

שם