תוכן עניינים

1. כללי

1.1 תרחיש הייחוס למתקפת סייבר על מערכות רכבת ישראל כתוצאה מתקיפת שרשרת האספקה, יכול להתממש באמצעות ערוצי תקיפה מגוונים ביותר, כגון חדירה למערכות של ספק בעל רמת הגנה נמוכה יחסית ודרכו חדירה למערכות החברה; שימוש בעדכוני תוכנה לגיטימיים להפצת נוזקה וכו'.

1.2 תרחיש הייחוס אינו מפרט איומים תיאורטיים, אלא מבוסס ניתוח המסתמך על מספר רב של אירועים שהתרחשו בארץ ובעולם, שמהותם היא פגיעה בארגונים, תוך ניצול שרשרת האספקה שלהם.

1.3 פעילותה השוטפת של חברת רכבת ישראל מערבת ספקים חיצוניים רבים, המספקים לה שירותים שונים. במסגרת השירותים ספקים אלה עשויים ליצור ולקבל מידע מ/עבור רכבת ישראל, לספק תשתיות לאחסון ועיבוד המידע, או לקבל גישה לרשת רכבת ישראל ולמידע שלה.

1.4 נכסי המידע של רכבת ישראל מסווגים כמידע פומבי/ פנימי/ רגיש עסקי/ רגיש אישי, ודליפתם לגורמים בלתי מורשים עלולה לגרום לסיכון ביטחוני או לנזק עסקי, תדמיתי או משפטי משמעותי לרכבת ישראל.

1.5 על-מנת למזער את הסיכונים לפגיעה בסודיות, באמינות ובזמינות המידע, נדרש להגן על נכסי המידע, הן כאשר הם מצויים על גבי ברשת רכבת ישראל והן כאשר הם מצויים אצל הספקים או באחריותם.

1.6 מסמך זה יפרט הנחיות ודרישות אבטחת מידע לספקים שיוצרים, מעבדים ו/או מחזיקים מידע של רכבת ישראל בתשתיות המחשוב שלהם.

1.7 נספח זה אינו עוסק בנושא חיבור מרחוק לתשתית המערכות החיוניות ולמערכות הבקרה ברכבת ישראל.

1.8 פירוט הדרישות ותיאור תהליך אישור חיבור ספקים חיצוניים למערכות פנימיות של רכבת ישראל, מפורט בנוהל "חיבור מרחוק של קבלנים חיצוניים למערכות של רכבת ישראל לצרכי תמיכה".

1.9 מסמך זה מהווה נספח סייבר בהתקשרויות הרכבת עם ספקיה.

2. הגדרות

2.1 "**ספק**": גוף חיצוני- על כל עובדיו וספקי המשנה שלו, המספק לרכבת ישראל שירותים (לרבות שירותי מיקור חוץ-Outsourcing), או טובין, באשר הם.

2.2 "**סייבר**" ("**המרחב הקיברנטי**"): המתחם הפיזי והלא פיזי שנוצר, או מורכב, מחלק, או מכל הגורמים הבאים: מערכות ממוחשבות, רשתות מחשבים ותקשורת, טכנולוגיה תפעולית (OT), תוכנות, מידע ממוחשב, תוכן שמועבר באופן ממוחשב, נתוני תעבורה ובקרה, לרבות הרובד האנושי. (האנשים המשתמשים בכל אלה).

2.3 "**הגנת סייבר**": כל הפעולות שתכליתן להגן על נכסי המידע של רכבת ישראל במרחב הסייבר.

2.4 "**מתקפת סייבר**": תקיפה במרחב הסייבר המסכנת נכסי סייבר, מערכות ותשתיות הנתמכות על ידם.

2.5 "**אירוע סייבר**": התרחשות אשר מעידה על פגיעה אפשרית בפעילותו התקינה של נכס סייבר, שקיים יסוד להניח, כי היא נובעת מפעילות מכוונת במרחב הסייבר.

2.6 "**נכנס מידע**": קובץ, רשומה, מאגר נתונים או עותק פיזי, המכיל מידע שנוצר או התקבל במסגרת הפעילות השוטפת של החברה, ובעל ערך לתפקודה התקין של רכבת ישראל.

2.7 "**מידע מוגן**[1]": כל אחד מאלה:

2.7.1 מידע שחוק הגנת הפרטיות, תשמ"א 1981, חל עליו.

2.7.2 מידע אודות ארגון שאינו נחלת הכלל.

2.7.3 סודות מסחריים לפי חוק עוולות מסחריות, תשנ"ט- 1999.

2.8 "**נכס סייבר חיוני**"נכס סייבר אשר תפקודו התקין נדרש לשם הבטחת רציפות תפקודה של רכבת ישראל כנכס סייבר לאומי- חיוני במדינת ישראל. בהגדרה זו נכללים: מערכות התפעול, מערכות בקרה תעשייתיות (ICS[2]), רשתות מחשבים חיונית לתפעולה השוטף של רכבת ישראל בשגרה ובחירום. בנוסף, בהגדרה זו נכללים כל נתון ו/או מידע (לרבות תכתובת), הקשורים למערכות אלו.

2.9 "**סביבת המידע של רכבת ישראל" (אצל הספק):** נכסי המידע של רכבת ישראל וכל התשתיות, תחנות הקצה והרכיבים המאפשרים גישה אליהם, או שבהם הם נוצרים, נשמרים, מעובדים או מועברים.

2.10 "**צורך עסקי**": הצורך הנובע מתפקיד העובד ו/או מהמשימות המוטלות עליו לצורך ביצוע השירותים עבור רכבת ישראל.

2.11 "**סודיות" (Confidentiality):** דרישה שהגישה למידע תוגבל אך ורק לגורמים שהוגדר שתפקידים מחייב גישה זו, וניתנו להם הרשאות בהתאם.

2.12 "**שלמות ואמינות" (Integrity):** דרישה שהמידע יהיה שלם, אמין ומדויק לכל אורך מחזור חייו.

2.13 "**זמינות" (Availability):** דרישה שהמידע יהיה זמין למשתמשים המורשים כאשר הם זקוקים לו.

2.14 "**תווך מאובטח" (Secure Channel):** יצירת תוואי תקשורת מאובטחת למניעת התערבות, צפיה בלתי מורשית ואו שיבוש נתונים.

2.15 "**הצפנה**": יישום של קריפטוגרפיה הממירה מידע גלוי (Clear Text) למידע מקודד (Cipher Text), באופן שיוכל להיות מפוענח ומובן אך ורק לגורמים מורשים.

2.16 "**HLD**": תכנון פתרון מותאם לאתרי/מערכות הלקוח ובחינת היתכנות של הפתרון ברמת ארכיטקטורה, היבטי סייבר, תשתיות תקשורת, רכיבי חומרה, ציוד, אביזרים, ממשקים, תוכנה ותצורת מערכת.

2.17 "**LLD**": תכנון ארכיטקטורה מעמיק, רשימות ציוד ויצרנים, אפיון מפורט של הממשקים ותוכנית המימוש.

2.18 "**אמצעי זיהוי**": אמצעי המספק פרטים לגבי זהותו של אדם, או מערכת, בעת ניסיון כניסה ואישור ביצוע פעולות מטעמם למערכת מידע.

2.19 "**גישה מרחוק**": התחברות משתמשים וספקים מחוץ לתשתית הארגון לטובת קבלת גישה למערכות/שרתי /תחנות קצה וכו' והקבצים שבהם

---

[1] הגדרת מערך הסייבר הלאומי

[2] "**מערכת בקרה תעשייתית**": (ICS-Industrial Control System) מערכת מבוססת מחשוב, המנטרת ומבקרת תהליכים המתחוללים בתוך מערכת יצור תעשייתית.

השייכים לרכבת ישראל, לצורכי עבודה של משתמשי הארגון ותחזוקה המבוצעת ע"י ממשקים עסקיים (ספקים/קבלנים).

3. אבטחת מידע

3.1 **סודיות והגנה על פרטיות**

3.1.1 הספק מצהיר שידוע לו כי מידע ומסמכים שימסרו לו ו/או למי מטעמו, על ידי רכבת ישראל במהלך מתן השירות לפי הסכם זה, מוגדרים כ"רגישים" ואין לפרסמם, או לעשות בהם שימוש, אלא לצורך מתן השירות עפ"י ההסכם.

3.1.2 הספק מתחייב לשמור בסוד ולא להעתיק, להודיע, למסור, או להביא לידיעת כל אדם כל ידיעה שתגיע, או שהגיעה אליו ו/או למי מטעמו, תוך כדי, או עקב ביצוע השירותים.

3.1.3 הספק מתחייב לשמור על סודיות המידע והמסמכים המפורטים לעיל, גם לאחר תום תקופת ההתקשרות, בהתאם להסכם זה.

3.1.4 הספק מתחייב להחתים את עובדיו ונותני השירותים מטעמו לרבות קבלני המשנה על הצהרת התחייבות לשמירת סודיות מתאימה וטופס העדר ניגוד עניינים, בהתאם לדרישות רכבת ישראל.

3.1.5 אין להעתיק, לפרסם, להעביר, להודיע, למסור, או להביא לידיעת כל אדם אחר, בין אם במישרין ובין אם בעקיפין, בין אם במעשה ובין אם במחדל, כל פריט מהמידע ו/או הסודות המקצועיים של רכבת ישראל אשר יגיע לידיו, לרשותו, או לידיעתו, באופן ישיר או עקיף, בקשר למתן השירות.

3.1.6 הספק מתחייב לשמירת סודיות באשר לכל הידע, שיטות העבודה, הציוד, המכשור, תצורת (קונפיגורציית) הרשת ומערך הגנת הסייבר, פרטי ומבנה הציוד המחשובי לרבות היצרנים והדגמים, הרכיבים וההתקנים, לרבות היצרנים והדגמים המצויים ברכבת ישראל, או שרכבת ישראל שוקלת את השימוש בהם בעתיד.

3.1.7 הספק מתחייב להביא את הוראות ההסכם והוראות סעיף זה לידיעת כל האנשים המועסקים על ידו, לשם ביצוע הסכם זה ו/או בקשר עמו.

3.1.8 הספק מתחייב למלא אחר כל הנחיות אגף הסייבר, הנחיות האבטחה והביטחון שיינתנו על ידי אגף ביטחון וחירום ברכבת ישראל וכן בהתאם לצורך, הנחיותיו של כל גורם מוסמך אחר ברכבת ישראל. (למען הסר ספק - רכבת ישראל לא תישא בעלויות יישום הנחיות אלו). האמור בסעיף זה הינו בכפוף לחובותיו הרגולטוריות של הספק.

3.1.9 הספק, עובדיו ונותני השירותים מטעמו מתחייבים להשתתף (במידת הצורך) בהדרכת/תדריך הגנת סייבר, שתוכנה יקבע על ידי אגף הסייבר ברכבת ישראל, עד פעם בשנה.

3.2 **דרישות כלליות**

3.2.1 הספק יתחייב לממש במלואם את התנאים העיקריים להלן:

3.2.2 הספק מתחייב לעמוד ולציית בכל הוראות חוק המחשבים, תשנ"ה-1995 וחוק הגנת הפרטיות, תשמ"א-1981 והתקנות שתוקנו מכוחו; וכן לציית לתנאים ותקנות עתידיים בנושא טיפול במערכות מידע ממוחשבות.

3.2.3 הספק מתחייב במסמך זה להיערך לפני תחילת מתן השירותים, למלא אחר כל דרישות והנחיות אגף הסייבר המפורטות בנספח זה, לרבות הנדרש בחוק הגנת הפרטיות, ובתקנות שהותקנו מכוחו מנותן שירותים חיצוני וממחזיק מאגרים מוגנים וממחויבויות רכבת ישראל, מכוח חוקי המדינה והוראות גורמי ההנחיה.

3.2.4 הספק יתחייב לניהול שוטף ומבוקר של השירותים הנדרשים, באופן מאובטח וממודר ולמניעת הגישה הפיזית לתחנות העבודה, לחדרי השרתים ולתשתית התקשורת המשמשת לעבודה מול רכבת ישראל-לגורמים שאינם מורשים.

3.2.5 ימונה נאמן הגנת סייבר מטעם הספק, אשר יונחה ע"י אגף הסייבר ברכבת ישראל ויהווה איש קשר(POC) לנושא ההגנה במרחב הסייבר.

3.2.6 הספק יעניק לנאמן הגנת הסייבר את כל הסמכויות, הכלים והאמצעים הנדרשים לביצוע תפקידו, לרבות סמכויות אכיפה על עובדי הספק בתחום הגנת הסייבר, והכל בכפוף להוראות והנחיות רגולטוריות החלות על הספק.

3.2.7 הרכבת תהיה רשאית להגדיר דרישות נוספות ו/או חלופות נוספות אל מול הספק.

3.3 <u>הגנה על נכסי סייבר חיוניים ותשתית IT ו- OT</u>

3.3.1 לא תותר התחברות ישירה, או ניסיון להתחברות ישירה של טכנאים ונציגי ספקים אל מערכות חיוניות (נכסי סייבר חיוניים, כהגדרתם ע"י רכבת ישראל).

3.3.2 ככלל, לא יאושר חיבור מרחוק לתשתית המערכות החיוניות ולמערכות הבקרה ברכבת ישראל. מקרים חריגים ייבחנו בנפרד, על פי צורך ע"י יחידת הסייבר ברכבת ישראל.

3.3.3 בכל רכש המיועד לרשתות, אמצעי הגנה (מסוג חומרה ותכונה), תשתית מערכות חיוניות, ומערכות הבקרה התעשייתיות ברכבת ישראל, יהיו כפופים לאישור אגף הסייבר ברכבת ישראל.

3.3.4 רכיבי תוכנה- ייבדק הצורך בביצוע מבדקי חוסן/חדירות טרם התקנתם, בהתאם להנחיות מחייבות, אשר יועברו ע"י אגף הסייבר ברכבת ישראל.

3.3.5 על הספק להתחייב לדווח בכתב ובאופן מיידי, למרכז הניטור הקיברנטי ברכבת ישראל בטלפון: 08-6533065 אודות כל התרחשות חריגה במתחמי הספק ו/או פגיעה, או ניסיון לפגיעה, ברכיבי האבטחה, גניבה, או ניסיון לגניבה של רכיבים המתוכננים להתקנה במערכות הקריטיות (נכסי סייבר חיוניים).

3.3.6 לא יתאפשר חיבור מחשבים, טלפונים, מצלמות, רכיבי זיכרון נייד (Disk On Key), או כל אמצעי מחשוב, או אחסון אחר, אל מערכות חיוניות ומערכות בקרה תעשייתיות(ICS), לרבות לצורך טעינת מכשירים סלולאריים/אחרים. במקרה הצורך ולאחר קבלת אישור פרטני-מראש ע"י מנהל אגף הסייבר ברכבת ישראל, יותר שימוש חד-פעמי ברכיב זיכרון נייד ייעודי ו/או מחשב נייד ייעודי.

3.4 <u>ניהול אבטחת מידע, רגולציה ותקינה- דרישות חובה</u>

3.4.1 בהתאם ללוח הזמנים והנחיות נוספות שיקבל הספק מנציגי הרכבת הספק יגדיר מדיניות אבטחת מידע התואמת חוקים, רגולציות ותקנים רלוונטיים לגביו, ההולמת את הסטנדרטים המקובלים בתחום.

המדיניות תאושר ע"י דרג ניהולי בכיר ותוטמע בקרב כל הגורמים בעלי גישה לסביבת המידע של רכבת ישראל.

3.4.2 לספק קיימים נהלי אבטחת מידע לכל הפחות בנושאים הבאים:

3.4.2.1. אירועי אבטחת מידע, ניהול תגובה, תחקור וכו';

3.4.2.2. אבטחה מידע במשאבי אנוש וניהול מחזור חיי עובדים (קבלה, עזיבה, הדרכות וכו');

3.4.2.3. אבטחת נכסי מידע של לקוחותיו;

3.4.2.4. אבטחת יישומים של הלקוח;

3.4.2.5. פיתוח מאובטח ותחזוקה של המערכות.

3.4.3 ככל ורלוונטי, הספק נדרש לעמידה מלאה בתקן PCI-DSS.

3.5 <u>אבטחת מידע במשאבי אנוש-דרישות חובה</u>

3.5.1 הספק אחראי לבצע בדיקות רקע לעובדיו המורשים לסביבת המידע של רכבת ישראל, בכפוף למגבלות החוקים הרלוונטיים (לדוגמא, הנחיות משטרת ישראל, תעודת יושר, בדיקות רקע פנימיות של רכבת ישראל או כל בדיקה אחרת המאושרת כל על ידי רשויות החוק).

3.5.2 הספק יבצע פעילויות להעלאת מודעות עובדיו לנושאי אבטחת מידע, הגנת הפרטיות ולסיכונים הרלוונטיים לביצוע תפקידם בפרט. על הספק לוודא את בקיאות עובדיו בנושאים אלו, בין היתר על ידי מבחני אפקטיביות שתוצאותיהם יועברו אל רכבת ישראל.

3.5.3 הספק יוודא ביטול הרשאות והחזרת ציוד ומצעי מידע שמכילים מידע של רכבת ישראל, בעת עזיבת עובד או שינוי תפקיד.

3.6 <u>העברת מידע רגיש/חסוי בין הספק ורכבת ישראל- דרישות חובה</u>

3.6.1 מידע דיגיטלי לא יועבר באמצעות רשת האינטרנט או במייל רגיל בין הספק ורכבת ישראל או בין הספק וספקי משנה, אלא בערוץ מאובטח, כפי שיימסר במועד ההעברה ע"י איש הקשר של הספק ברכבת ישראל.

3.6.2 מידע על-גבי אמצעים פיזיים (עותק קשיח, מדיה נתיקה) יימסר ישירות לידי עובד רכבת ישראל או בתהליך שיוגדר במועד העברה ע"י איש הקשר של הספק ברכבת ישראל.

3.6.3 יש להצפין מידע המועבר על-גבי מדיה נתיקה. מפתח הצפנה יימסר בנפרד לצד המקבל.

3.6.4 בעת העתקת מידע למדיה נתיקה ע"י ספק משנה, יש לוודא מחיקה אפקטיבית של כל העותקים מתשתיות המחשוב של ספק המשנה.

3.7 <u>אחסון מידע- דרישות חובה</u>

3.7.1 ככלל, המידע של רכבת ישראל יאוחסן בשרתים ברשת הפנימית של הספק, ולא בתחנות הקצה.

3.7.2 במקרים בהם החומרים הוגדרו רגישים ע"י רכבת ישראל כלל המידע יישמר באופן מוצפן וזאת ע"י אמצעי ותקני הצפנה מקובלים.

3.7.3 במקרים בהם יש צורך עסקי לשמור מידע רגיש של רכבת ישראל במחשב נייד, יש להצפין את הקבצים או את הכונן הקשיח של המחשב.

3.7.4 בסיום ההתקשרות עם רכבת ישראל, הספק יוודא העברת כל המידע לרכבת ישראל ומחיקה לצמיתות של כל ההעתקים שלו משרתי הספק. יש לשמור תיעוד (לוג) של מחיקת המידע. האמור בסעיף זה כפוף לחובותיו הרגולטריות של הספק.

3.8 **<u>גיבוי והתאוששות- דרישות חובה</u>**

3.8.1 הספק יהיה אחראי לגיבוי המידע של רכבת ישראל. גיבויים הכוללים מידע רגיש יישמרו בצורה מאובטחת, מוגנים מפני שכתוב ויוצפנו. הגישה אליהם תתאפשר רק בהתאם לצורך עסקי מוצדק

3.8.2 יש לאחסן את מפתחות ההצפנה לגיבויים בנפרד מהמדיה.

3.8.3 הספק יתחזק תכניות המשכיות עסקית והתאוששת מאסון, אשר תתמוך בהמשך הפעילות העסקית עבור נכסי ומערכות רכבת ישראל.

3.9 **<u>ביצוע סקרים, שרשרת אספקה-דרישות חובה</u>**

3.9.1 כאשר יידרש לכך ע"י אגף הסייבר, הספק יתחייב לעמוד בדרישות שאלון שרשרת האספקה של מערך הסייבר הלאומי, וזאת ע"פ הקטגוריה הרלוונטית (לדוגמא, מחשבון ענן, Hosting, ניהול אבטחת מידע וכדומה).

3.9.2 בהתאם לנספח זה, רשאית הרכבת לערוך סקר סיכונים, או באמצעות צד ג' ללא כל עלות נוספת.

3.9.3 הספק מתחייב לאפשר לנציגי הרכבת לבצע ביקורת מערכי אבטחה, במשך שעות העבודה המקובלות וללא התראה מוקדמת, במתקניו, אשר להם זיקה, או השפעה על אבטחת המערכות המשמשות את רכבת ישראל ללא כל עלות נוספת.

3.9.4 הרכבת, או נציגיה המוסמכים, יהיו רשאים לבצע בדיקות מערכי אבטחה, בקרת חסינות, איתור פרצות אבטחה ובדיקת יעילותם של מנגנונים המשמשים לאבטחת המערכות המשמשות את רכבת ישראל ללא כל עלות נוספת.

3.9.5 על הספק לערוך בדיקות אבטחה סמויות ממערכים חיצוניים לספק, לבדיקת ההגנות בפני גישה חיצונית ממערכות הספק, או ממערכות חיצוניות לספק, אל מערכות רכבת ישראל, נשוא ההתקשרות.

3.9.6 רמת הכיסוי של הסקרים תותאם לרגישות המידע ולרמת הסיכון הנשקף לרכבת ישראל, מאופי הפעילות מול הספק ותכלול בדיקות שמטרתן לוודא את עמידת הספק בדרישות הגנת סייבר ולזהות חשיפות לסיכונים אלו.

3.9.7 רכבת ישראל רשאית לדרוש תיקון ליקויים, אשר יתגלו בסקרי סיכונים, ביקורות מתוכננות, ביקורות פתע, גילוי אקראי, או יזום של ליקויי אבטחה במתקני הספק- והספק יחויב לתקן ליקויים אלו, תוך פרק זמן סביר (לעניין זה - הזמן המוערך ע"י גופים מקצועיים לתיקון הליקוי) וללא כל עלות נוספת.

3.9.8 במידה וימצאו ליקויים קריטיים המשפיעים על רמת הגנת הסייבר של מערכות רכבת ישראל, יידרש הספק לתקן ליקויים אלו באופן מיידי וללא כל עלות נוספת.

3.10 **<u>דו"חות בקרה-דרישות חובה</u>**

3.10.1 הספק מתחייב להעביר לרכבת ישראל לפי דרישה, או בהליך שוטף דו"חות בקרה, אשר נדרשו במסמכי ההתקשרות ודו"חות נוספים

על-פי הצעתו של הספק, ללא חיוב נוסף. בין הדו"חות יכללו:

3.10.1.1. דו"חות על מערכת ההרשאות (הרשאות למשתמש, משתמשים בקבוצת משתמשים, וכו')

3.10.1.2. דוחות ממערכת הניטור (Auditing), לרבות: מספר אירועים מכל סוג, ניסיונות גישה כושלים, וכו'.

3.10.2 קבצי הדוחות יתאימו ככל הניתן לתוכנות חיצוניות אחרות ובפורמטים מקובלים כגון XML, Doc, TXT, וכו'.

3.11 **<u>גישה מרחוק-דרישות חובה</u>**

3.11.1 ככלל, לא תתאפשר לספק כל גישה מרחוק למערכות רכבת ישראל.

3.11.2 על אף האמור בתתי הסעיפים לעיל, תותר הקמת תווך בין מתחמי הספק לבין רכיבים ממערכות רכבת ישראל, רק אם יתקיימו התנאים הבאים:

3.11.2.1. החיבור יבוצע אך ורק ממחשבי קצה שהספק יעביר לרכבת ישראל, מחשבים אלו יוקשחו ע"י רכבת ישראל.

3.11.2.2. הקמת התווך נבחנה ואושרה על ידי אגף הסייבר ברכבת ישראל, לאחר שנבחן הצורך/הכורח שבהקמת התווך, נבחנו הסיכונים שבהקמת התווך והבקרות המפצות.

3.11.2.3. הגישה מרחוק תהיה מוגבלת רק לרכיבים אליהם קיימת חובת התחברות מרחוק.

3.11.2.4. הגישה מרחוק תהיה מוצפנת (בהתאם לדרישות המצוינות בסעיף "הצפנה")

3.11.2.5. יוגדרו פרקי זמן של חוסר פעילות שלאחריהם תתנתק הגישה (Session Timeout).

3.11.2.6. גישה מרחוק תבוקר ותוגבל לעובדים של הספק אשר יאושרו ע"י רכבת ישראל מראש, כאשר לכל עובד יהיה שם משתמש אישי. היה ולא ניתן להגדיר שם משתמש אישי, יוגבלו הרשאותיו של המשתמש הקבוצתי לפעולות של ניטור ואתחול בלבד ולא תותר כל התקנה, או עדכון של רכיב תוכנה-באמצעות גישה מרחוק.

3.12 **<u>קניין רוחני- דרישות חובה</u>**

3.12.1 כל התוכנות ומערכות המחשוב אשר משמשות את הספק במתן השירותים לרכבת ישראל, עומדות בדרישות הדין בתחום הקניין הרוחני, רישיונן תקף ולספק זכות שימוש בהן.

3.12.2 לא יעשה שימוש בתוכנות וציוד אשר אינם נתמכים עוד על ידי היצרן ואשר הוגדרו על ידו כ-End Of Life.

4. ביטחון ואבטחה פיזית

4.1 הספק ימלא את כל דרישות הרכבת בנוגע לאבטחת מידע, לרבות דרישות פרטניות לאבטחה פיזית, אבטחת סביבת מחשוב, הגנה על מסמכים וציוד במתקניו ולתהליכי בדיקות מהימנות לעובדיו.

4.2 הגישה הפיזית לסביבת המידע של רכבת ישראל תוגבל לבעלי צורך עסקי בלבד. הסביבה תהיה מוגנת מפני גישה של גורמים בלתי מורשים באמצעות מערכות בקרת גישה וכניסה.

4.3 כל הרכיבים וההתקנים בהם מאוחסן ומעובד המידע של רכבת ישראל יהיו מוגנים מפני נזקים סביבתיים (הצפה, שריפה וכדומה).

4.4 הספק יתחייב לניהול רשימת נותני שירותים עדכנית, של בעלי גישה למידע, או לתחנות העבודה ברכבת ישראל, לרבות תפקידיהם וסמכויות הגישה למידע, כפי שהוגדרו ע"י וכן דווח על כל שינוי לרכבת. רשימת נותני השירותים תאושר ע"י הרכבת טרם העסקת העובדים במתן השירותים, נשוא ההתקשרות.

4.5 היה ורלוונטי, הספק יתכנן ויממש מענה ביטחון ואבטחה לכלל הפרויקט, החל משלב קבלת צו התחלת עבודה הראשון בפרויקט ועד סיום העבודות ומסירת המערכת לרכבת ישראל וכן בתקופת התחזוקה.

4.6 המענה יהיה בהתאמה לדרישות האבטחה והביטחון של רכבת ישראל, יעמוד בתקנים המחייבים ובתקנות הרלוונטיות של מדינת ישראל, משטרת ישראל, משרד התחבורה, משרד התשתיות והמשרד לביטחון פנים.

4.7 המענה יתוכנן לכלל הפרויקט וימומש בהתאם לתכנית המימוש ושלבי הפרויקט שהוגדרו במסמך זה ויוגדרו בהתאם להתפתחות הפרויקט על ידי רכבת ישראל.

4.8 התכנית תותאם למענה הביטחון והאבטחה הקיים כיום ברכבת ישראל ותאושר על ידי אגף ביטחון וחרום ברכבת ישראל, טרם יישומה.

4.9 הספק יציג פתרון למניעת גישה למרכיבי מערכת בתחזוקת הציוד, להגנתו ולבקרתו.

5. אירועים חריגים

5.1 הספק ינהל דו"חות איתור ומעקב אירועים חריגים, דיווח וטיפול בהם.

5.2 הספק, או נאמן ההגנה בסייבר מטעמו (ראה סעיף 3.2.5 לעיל), ידווח על כל ליקוי אבטחת-מידע, שיגלה במערכות הספק, תוך לא יותר מ48 שעות מרגע גילוי האירוע.

5.3 ליקויים מהותיים הנוגעים בין במישרין ובין בעקיפין למערכות רכבת ישראל ו/או למערכות- נשוא ההתקשרות, **ידווחו במיידית למרכז הניטור הקיברנטי ברכבת ישראל בטלפון: 08-6533065**

5.4 מחויבות הספק לשיתוף פעולה באירועי סייבר:

5.4.1 בכל אירוע בו מעורב אחד מעובדי הספק, או ממשקיו העסקיים, או שקיים חשד למעורבות שיש עמה השלכה ישירה, או עקיפה על רמת ההגנה בסייבר ברכבת ישראל, או בטחון האינטרסים של רכבת ישראל.

5.4.2 בכל הפרה, או חשד להפרה של חוקים, הנחיות גורמי ההנחיה, תקנות, או נהלי הגנת הסייבר.

5.4.3 בחקירת אירועים, או חשדות, לחריגות אבטחה.

6. קניין/זכויות בחומר

6.1 מוצהר בזאת כי לספק אין ולא תהיינה כל זכויות בחומר שיועבר לידיו על ידי רכבת ישראל לצורך ביצוע השירותים לפי הסכם זה והספק יהיה רשאי לעשות שימוש בחומר כאמור, אך ורק במסגרת ולשם ביצוע השירותים ובהתאם לכל יתר הוראות הסכם זה.

6.2 מוצהר בזאת כי רכבת ישראל תהיה בעליו היחידים של כל הזכויות בכל חומר שיתקבל, ייאסף, יוכן ויעובד על ידי הספק במסגרת מתן השירותים לפי הסכם זה, לרבות הדיווחים שהספק מעביר לרכבת ישראל. רכבת ישראל תהיה רשאית לעשות בחומרים כאמור כל שימוש שתמצא לנכון, בכפוף להוראות כל דין.

6.3 הספק יצהיר כי הוא מוותר על זכותו לתבוע כל זכות קניינית מרכבת ישראל ובכלל זה את הזכות לקניין רוחני.

7. אי עמידה בדרישות נספח זה

7.1 אי עמידה בדרישות נספח זה, כמוה כהפרה יסודית של הסכם ההתקשרות בין הספק לרכבת, ולרכבת כל התרופות הקנויות לה על פי דין ועל פי מסמכי ההתקשרות. בעת הפרת סעיפי ההתקשרות בנספח זה, תהיה רכבת ישראל רשאית:

7.2 להפסיק באורח חלקי, או מלא את הפעלת המערכת, או השירותים, נשוא ההתקשרות, משיקוליה היא ולדרוש מהספק שיפוי מלא על הנזקים שיגרמו כתוצאה מפעולה זו.

7.3 בכל מקרה יתבע הספק לתקן את הליקויים באורח מיידי ועל חשבונו, לאור הפרת ההסכם.

7.4 בנוסף על הרשום לעיל תהיה נתונה בידי רכבת ישראל הזכות לדרוש מהספק לשאת בעלות סקרי הסיכונים, שיבוצעו ע"י רכבת ישראל, בגין אי עמידת הספק במחויבויותיו, כנדרש לעיל.

8. סיום התקשרות

8.1 עם סיום ההתקשרות עם הספק, על הספק לבצע את הפעולות הבאות:

8.2 להחזיר לרכבת ישראל, או לכל גורם מטעמה את כל הרשומות, המדיה, האמצעים, הציוד והרכיבים השייכים לרכבת ישראל- בהם עשה שימוש לצורך עבודתו.

8.3 הספק מתחייב להשמיד כל מידע השייך לרכבת ישראל המצוי ברשותו ואשר לא יימסר לרכבת והכל בכפוף לקיומן של הוראות והנחיות רגולטוריות החלות על הספק.

8.4 הספק יתחייב כי לא נשארו ברשותו כל מסמכים, מידע, או פריטים הנוגעים למערכות הקריטיות.

8.5 הספק יוודא כי הדיסקים הקשיחים אשר הכילו מידע של רכבת ישראל נמחקים בהתאם להוראות תקן FIPS SP 800-88 - Guidelines for Media Sanitation, כאשר יש להתייחס לכל פריט מידע כ"מידע רגיש".

8.6 היה והספק נדרש להמשיך ולהחזיק פריטים כנ"ל, יידרש לחתום על הצהרה בה הוא מתחייב להעביר כל מידע ורכיב הנוגע למערכות קריטיות, רק לגורם מורשה מטעם רכבת ישראל ולאחר קבלת אישור כתוב ממנהל אגף הסייבר ברכבת ישראל (ממונה תמ"ק-רכבת ישראל).