נספח א'
מפרט איפיון השירותים

כללי

חברת רכבת ישראל בע"מ (**להלן: "המתאם"**) מבקשת לקבל הצעה מחברה הניגשת למכרז (**להלן: "הספק" או " המציע"**) למתן שרותי והפעלת אתר אינטרנט הכולל: שירותי אספקת בחירת מתנות והענקת שוברים (מצוינות, ימי הולדת וכיו"ב), עבור עובדי רכבת ישראל ובני משפחותיהם (**להלן: "השירותים"**).

המפרט המופיע בסעיף 2 מטה, מהווה רשימת מרכיבים (מרכיב אחד או מקבץ של מספר מרכיבים).

הרכבת שומרת לעצמה את הזכות ולהוסיף ולגרוע שירותים בהתאם לצרכי החברה.

סל 1 - בחירת ואספקת מתנות לחגים, לרבות הקמת חנות מקוונת לבחירת מתנות ואספקת המתנות לבית העובד

1. המציע יספק מתנות לעובדים לחגים, ימי הולדת ועל פי שיקול דעתה הבלעדי של הרכבת, לפי עלות קבועה מראש ובהתאם להצעת המציע במכרז.
2. המתנות יוזמנו בחגים ראש השנה ופסח, בכמויות משתנות ובהיקפים משתנים הכל בהתאם למספר העובדים הזכאים למתנות ולשווי המתנות לו הם זכאים, באופן ובמועד שיידרש על ידי נציגי הרכבת המוסמכים לבצע הזמנות מכוח מכרז זה ובהתאם לשיקול דעת הרכבת, צרכיה ותקציבי.
3. נכון למועד פרסום המכרז קיימות 4 דרגות של תקציב המתנות לחגים. יובהר, כי הרכבת אינה מתחייבת להיקף הרכישה ולתקציב המתנות והוא תלוי בתקציב הרכבת ובמצבת העובדים, אשר עשויים להשתנות בכל עת.
4. <u>דרגות המתנות לחגים</u>:
   - 4.1. מתנה אחת בערך מלא.
   - 4.2. 2 מתנות בסה"כ ערך מלא – שווי כל מתנה יהיה חמישים אחוז מערך המתנה המלא.
   - 4.3. מתנה בתוספת תשלום של העובד – מתנה בערך מלא בתוספת תשלום של העובד בכרטיס אשראי).
   - 4.4. מתנת וועד.

   יודגש כי לרשות הרכבת עומדת הזכות לשנות את שווי המתנה, מעת לעת, בהתאם לשיקול דעתה הבלעדי.
5. <u>מגוון מוצרים</u>
   - 5.1. המתנות שיוצעו יהיו מגוונות ויכללו לכל הפחות את חמשת הקטגוריות הבאות: מוצרי חשמל, טקסטיל ומוצרים לבית, כלי בית ובישול, מולטימדיה וטכנולוגיה, תיירות ומוצרי נופש וכיו"ב.
   - 5.2. מתנה גדולה (בשווי מלא) ומתנה קטנה (בשווי חלקי – 50% מהסכום) המציע יציע 2 מתנות לפחות בכל אחת מהקטגוריות המצוינות בסעיף 2.5.1 ובכל שווי מתנה.

5.3. מתנה גדולה בתוספת תשלום של העובד באמצעות כרטיס אשראי – יוצעו לבחירה 6 מתנות לכל הפחות.

5.4. מתנת וועד (170 ₪) – יוצעו לבחירה 6 מתנות לכל הפחות.

6. על המציע לתת אפשרויות להחלפה ו/או שדרוג המתנה לעובד לפי בחירתו בהיקף של 40% מסך המתנות המוצעות בכל קטגוריה.

7. במסגרת תקופת הפעילות המציע יקבל את הזמנות העובדים באמצעות אתר האינטרנט (החנות המקוונת) ויספק אותן לכתובות האספקה שהוגדרו מראש ו/או על ידי העובד בעת ביצוע ההזמנה (בית העובד, מתחמים, מחסנים, מנהלות משא"ן וכיו"ב) תוך פרק שנקבע מראש.

8. <u>אספקת תווי שי בחוזה נפרד</u>

לרכבת קיים הסכם נפרד לאספקת תווי שווי מסוג גיפט קארד. עובדי הרכבת יוכלו, במסגרת החנות המקוונות לבחירת המתנות לחגים שיספק המציע הזוכה, גם את האפשרות לקבל תווי שווי במקום מתנה אחת גדולה או לבחור לשלב תווי שי בשווי חלקי יחד עם מתנה קטנה. תווי השי יסופקו לעובדים ע"י הרכבת בהתאם לכמות שתיבחר באתר.

9. **<u>מפרט השירותים הנדרשים</u>**:

9.1. על הספק הזוכה להגיע אל משרדי הרכבת ולהציג לנציג הרכבת את אתר האינטרנט המוצע ואת מגוון המתנות המוצעות באתר לבחירה שלושה חודשים לפחות לפני תאריך ערב החג.

9.2. הפעלת אתר אינטרנט לבחירת מתנות (חנות מקוונת).

9.3. על הספק הזוכה להפעיל חנות מקוונת, שתהיה נגישה לעובדי הרכבת, הן במחשב והן במכשירי הסלולר, לצורך בחירת מתנות.

9.4. הספק הזוכה יתחזק את האתר באופן שוטף, לרבות:

9.4.1. שמירה על נראות אחידה וייצוגית של האתר, בהתאם לכללי המותג ולאישור המתאם, תוך שימת דגש על נוחות המשתמש.

9.4.2. תיקון תקלות טכניות ו"באגים" במערכת:

מס'	רמת תקלה	רמת שירות נדרשת (SLA)	
1.	תקלה קריטית (משביתת מערכת באופן מלא)	תחילת עבודת מתכנתים	רבע שעה (15 דקות) מפתיחת התקלה
		השלמת הטיפול וחזרה לפעילות מלאה	– עד שעתיים מפתיחת תקלה
2.	תקלה רגילה (משביתת מערכת חלקית)	תחילת עבודת מתכנתים	שעה אחת מפתיחת קריאה
		השלמת הטיפול וחזרה לפעילות מלאה	24 שעות מפתיחת תקלה
3.	תקלה בהוצאת הודעות sms	מתן פתרון חלופי	מידי עם פתיחת התקלה

9.4.3. שמירה על פעולה רציפה ותקינה של האתר.

9.4.4. POC לתמיכה במנהל המערכת בשעות העבודה המקובלות (א׳- ה׳ 08:00 - 17:00).

9.4.5. POC לתמיכה בתקלות - 24-שעות ביממה, בכל ימי הפעילות המוגדרים.

9.4.6. האתר יציע מתנות לעובדים על פי הקטגוריות ודרישת הרכבת כמפורט בסעיף 5 לעיל.

9.4.7. עובד הרכבת ייכנס לאתר באמצעות שם משתמש (מס׳ עובד) וסיסמא

9.4.8. יודגש כי למערכת תהיה אפשרות לשחזור סיסמא באמצעות SMS או דוא״ל.

9.4.9. באחריות הספק הזוכה לבצע מעקב ובקרה על ביצוע ההזמנות באתר וכן לשלוח תזכורות באמצעות דוא״ל, הודעות SMS וכד׳ לעובדים שטרם בחרו מתנה. בהתאם לדרישת המתאם ובאישורו בלבד.

9.4.10. תקופת זמן בחירת המתנה תיקבע מראש, בתיאום בין הספק הזוכה לנציג הרכבת.

9.4.11. בתום תקופת הזמן שהוקצבה לבחירת המתנה תיסגר הגישה לאזור בחירת המתנות ויועבר קובץ מסודר לנציג הרכבת לאישור סופי.

9.4.12. הקובץ יכיל פרמטרים שיוגדרו מראש לאתר הבחירה. הקובץ יועבר במייל ויהיה מוגן בסיסמא אשר תסוכם מראש בין הספק ונציג הרכבת (הסיסמא לא תירשם בגוף המייל).

9.5. <u>הפעלת מוקד שירות לקוחות</u>

הספק יפעיל מוקד שירות לקוחות למתן שירות לעובדי הרכבת גם במהלך בחירת המתנה וגם לאחריה (לעניין האחריות, קשר עם ספקי המשנה וכיו״ב). מוקד השירות יפעל בימים א׳-ה׳ בין השעות 09:00-16:00 לפחות.

9.6. המתנות אשר יציע הספק לפני כל חג יוצגו תחילה לנציגי הרכבת ויאושרו על ידם. מתנה שלא תאושר לא תוצע לעובדים והספק יציג מתנה חלופית באותו תחום.

9.7. הספק יציג את המתנות לבחירה באופן ברור באתר בליווי תמונה, מפרט טכני/וכל מידע רלוונטי , לרבות אפשרויות שווי המתנה, החלפה למוצרים/זיכוי כספי (במידה וניתן לבצע החלפה/לקבל זיכוי כספי).

9.8. אם נדרשת תוספת תשלום ע״י העובד בבחירת המתנה – יוצג הסכום המדויק לתשלום ואופן גביית התשלום.

9.9. במסגרת תקופת הפעילות יפעיל ויתחזק המציע את החנות המקוונת באופן שוטף, לרבות אחסון האתר בשרתים מאובטחים, גיבוי יומי למידע באתר, תיקון תקלות במערכת, שחזור האתר תוך 4 שעות במקרה של נפילת שרתים ו/או מתקפת סייבר ו/או כל תקלה משביתה אחרת, הפעלת מוקד שירות טלפוני ואחריות על פעולה רציפה של האתר.

9.10. **מתן הרשאת מנהל (ADMIN)**

9.10.1. הוצאת דו״ח מפורט לסטטוס ביצוע הזמנות, בזמן אמת.

9.10.2. הוצאת דו״ח משתמשים יומי/ שבועי/ חודשי/ שנתי.

9.10.3. צפייה במוצרים הנמכרים ביותר/ העמודים הנצפים ביותר/ עמודי הנטישה באתר.

9.11. **אספקת המתנות**

9.11.1. הספק הזוכה מתחייב להימצאות מלאי, לכל סוג מתנה, המאפשר לכל עובד לבחור ולקבל את המתנה המועדפת עליו

9.11.2. כל מתנה תארז בנפרד ובאופן מכובד.

9.11.3. לכל מתנה אשר הוצגה לה אפשרות החלפה יוצמד פתק החלפה ברשתות המתאימות.

9.11.4. לכל מתנה תוצמד תעודת אחריות.

9.11.5. בהתאם להחלטת המתאם תוצמד ברכה לכל מתנה. הספקת הברכות ועיצובן באחריות הרכבת.

9.11.6. אספקת המתנות תהא בכתובת בה בחר העובד לקבל את המתנה, לרבות ביתו, וזאת עד 3 ימים לפני ערב החג.

9.12. **לוחות זמנים נדרשים**

פעולה	לוח זמנים נדרש
הצגת אתר המתנות לנציגי הרכבת	שלושה חודשים לפני תאריך ערב החג
אישור האתר והמתנות לאחר הערות/בקשות	שבועיים מיום הצגת האתר לרכבת
העברת קובץ זכאים ע״י הרכבת לספק	שבועיים לפני עליית האתר לאוויר
עליית האתר לאוויר	חודשיים לפני תאריך ערב החג ביום פתיחת האתר לשימוש יפיץ הספק הודעה לעובדים באמצעות הדוא״ל ו-sms, לכלל העובדים שקיבל ברשימה שסופקה ע״י הרכבת, ובה קישור לאתר האינטרנט לבחירת המתנות והוראות לשימוש באתר.
משך זמן בחירת המתנה על ידי העובד	שבועיים מיום עליית האתר לאוויר, כל עוד האתר פעיל העובד יוכל לשנות את בחירתו
אישור דוחות סופיים	עד שבוע מיום סגירת האתר לבחירה
הפצה ואספקת המתנות	מיום אישור הדוחות ועד שלושה ימים לפני ערב החג

10. <u>העברת מידע בין הספק ונציגי הרכבת</u>

כל העברת מידע בין הספק ונציגי הרכבת, אשר מכיל מידע רגיש ופרטי עובדים יועבר בקבצים מוצפנים ומוגנים באמצעות סיסמא. הסיסמא תסוכם מראש בין הספק ונציג הרכבת ולא תירשם בגוף המייל.

11. **<u>פיצויים מוסכמים – סל 1</u>**

11.1. במידה והספק הזוכה לא יעמוד באיכות השירות וברמות השירות המוגדרות, ייגבו ממנו פיצויים מוסכמים כמופיע בקנסות בגין אי עמידה בתקני שירות.

11.2. **מנגנון קנסות בגין אי עמידה בתקני שירות**

רמת שירות נדרשת	החריגה	גובה וסוג הפיצוי
העברת רשימת מתנות אפשרית לחג - 3 חודשים לפני ערב החג	הצגת אתר ומגוון המתנות לבחירה פחות מ- 3 חודשים לפני ערב החג.	קנס של 1,000 ₪ בגין כל שבוע איחור.
אספקת המתנות לעובד במועד שנקבע	פיגור במועד אספקת המתנות.	קנס של 200 ₪ בכל יום איחור באספקה לכל עובד.
העברת קובץ הכולל פירוט בחירת העובדים הזכאים למתנה לאחר סגירת אתר הבחירה	איחור במועד העברת הקובץ.	קנס של 150 ₪ בגין כל יום איחור.
מלאי חסר של מתנות	מלאי חסר של מתנה.	קנס בסך 250 ₪ בגין כל הפרה, ועד 5,000 ₪ סך הכל.
תפעול תקין של אתר האינטרנט	תקלה טכנית הפוגעת ביכולת העובדים בשימוש באתר	קנס של 1,000 ₪ בגין כל יום בו התקלה לא מטופלת

12. שימוש במידע שיועבר ע"י הרכבת

12.1. הספק מתחייב שלא לעשות שום שימוש במידע שיועבר אליו ע"י הרכבת שלא למטרת אספקת השירותים לפי מכרז זה, ולא להעביר את המידע לצד שלישי.

12.2. הספק מתחייב למחוק כל מידע שהגיע לרשותו לאחר השלמת אספקת המתנות לעובדי בכל חג ולאחר אישור נציג הרכבת.

<u>סל 2 - אספקת שוברי מתנה</u>

מפרט השירותים הנדרשים - ניהול הוקרות , בחירת והענקת שוברים

1. **<u>כללי:</u>**

1.1. רכבת ישראל מעוניינת לרכוש מגוון שוברי מתנות לעובדים (להלן: "שוברים") בעבור עובדי רכבת ישראל.

1.2. הכרטיסים יאפשרו רכישת טובין ושירותים בפריסה ארצית במגוון בתי עסק בהתאם לקטגוריות רכישה (להלן: "קטגוריות") ובהתאם לתכולת שירותים שתקבע על ידי המתאם מטעם הרכבת (להלן: "המתאם") והכל בכפוף ובהתאם לאמור בנספח 2 למסמכי פנייה זו.

1.3. השוברים יוכלו להגיע באחת או יותר מהדרכים הבאות: שוברים מוחשיים, שוברים להדפסה ביתית ו/או שוברים דיגיטליים.

2. **<u>קטגוריות שוברים:</u>**

ביכולתו של המציע לספק מגוון שוברים מקטגוריות שונות ובמגוון בתי עסק שונים שיכילו לכל הפחות את הקטגוריות האמורות להלן:

2.1. **מסעדות** - המציע הזוכה יספק שוברים למגוון מסעדות. על המסעדות שיוצעו על ידי המציע לעמוד בקריטריונים שלהלן, במצטבר:

- המסעדות המוצעות תהינה בפריסה ארצית ותוצע לפחות מסעדה אחת בכל אחד מהאזורים הבאים: תל אביב יפו, מרכז, שרון, זיכרון יעקוב והסביבה, צפון, חיפה וקריות, ירושלים והסביבה, אשקלון, אשדוד, באר שבע ודימונה.
- מסעדות חלביות, מסעדות בשריות, מסעדות שף.
- במגוון המסעדות המוצעות תוצענה מסעדות כשרות ומסעדות כשרות למהדרין.

2.2. **ארוחות בוקר** - המציע הזוכה יספק שוברים למגוון בתי קפה/ מסעדות לארוחות בוקר. על בתי הקפה/ המסעדות שיוצעו על ידי המציע לעמוד בקריטריונים שלהלן, במצטבר:

- בתי הקפה/מסעדות המוצעים יהיו בפריסה ארצית ותוצע לפחות מסעדה אחת בכל אחד מהאזורים הבאים: תל אביב יפו, מרכז, שרון, זיכרון יעקוב והסביבה, צפון, חיפה וקריות, ירושלים והסביבה, אשקלון, אשדוד, באר שבע ודימונה.
- במגוון בתי הקפה/ מסעדות המוצעים יוצעו בתי קפה/ מסעדות כשרות ומסעדות כשרות למהדרין.

2.3. **בתי מלון, צימרים ותיירות כפרית** - המציע הזוכה יספק שוברים לאירוח במגוון בתי מלונות וצימרים בפריסה ארצית. על בתי המלון והצימרים שיוצעו על ידי המציע לעמוד בקריטריונים שלהלן, במצטבר:

- השובר יקנה לינה זוגית ללילה אחד וכן ארוחת בוקר זוגית.
- בכל ימות השבוע.
- בתי מלון ברמת 4 כוכבים ומעלה ומבחר צימרים יוקרתיים.

2.4. **קולנוע -** המציע הזוכה יספק שוברים לכרטיס יחיד או זוגי לסרט במגוון בתי קולנוע, בהתאם לקטגוריות הבאות:

2.4.1. קטגוריה 1 - **כרטיס יחיד לסרט**: על הסרטים שיוצעו לעמוד בקריטריונים שלהלן, במצטבר:

- השובר יקנה כניסה לסרט.
- הצפייה תאפשר בכל ימות השבוע.
- בתי הקולנוע המוצעים יהיו בפריסה ארצית ובעלי סניפים באזורים הבאים, לכל הפחות: תל אביב יפו, מרכז, שרון, זיכרון יעקוב והסביבה, צפון, חיפה וקריות, ירושלים והסביבה, אשקלון, אשדוד, באר שבע ודימונה.

2.4.2. קטגוריה 2- **כרטיס זוגי לסרט**: על הסרטים שיוצעו לעמוד בקריטריונים שלהלן, במצטבר:

- השובר יקנה כניסה זוגית לסרט.
- הצפייה תאפשר בכל ימות השבוע.

- בתי הקולנוע המוצעים יהיו בפריסה ארצית ובעלי סניפים באזורים הבאים, לכל הפחות: תל אביב יפו, מרכז, שרון, זיכרון יעקוב והסביבה, צפון, חיפה וקריות, ירושלים והסביבה, אשקלון, אשדוד, באר שבע ודימונה.

2.4.3. קטגוריה 3 - **כרטיס יחיד לסרט VIP**: על השירות שיוצע לעמוד בקריטריונים שלהלן במצטבר:

- השובר יקנה כניסה יחיד לסרט.
- הצפייה תאפשר בכל ימות השבוע.

2.4.4. קטגוריה 4 - **כרטיס זוגי לסרט VIP**: על השירות שיוצע לעמוד בקריטריונים שלהלן במצטבר:

- השובר יקנה כניסה זוגית לסרט.
- הצפייה תאפשר בכל ימות השבוע.

2.5. **ספא** – המציע יספק שוברים זוגיים לחבילות ספא ועל השירותים המוצעים על ידי המציע לעמוד בקריטריונים שלהלן, במצטבר:

- חבילת הספא הינה חבילה זוגית.
- החבילה תכלול לכל הפחות, שהיה במתחם ואפשרות לטיפול לבחירה לדוגמא עיסויי, פדיקור וכד'.
- אפשרות אתרי הספא לבחירה יהיו בפריסה ארצית ולכל הפחות במקומות הבאים: תל אביב- יפו, מרכז, שרון, זיכרון יעקוב והסביבה, צפון, חיפה וקריות, ירושלים והסביבה, אשקלון, אשדוד, באר שבע ודימונה.

2.6. **סדנאות וקורסים** - המציע יספק שוברים לסדנאות שונות, כדוגמת סדנאות בישול, סדנאות אפיה, סדנאות יין, סדנאות צילום, סדנאות שוקולד, סדנאות איפור וסדנאות סטיילינג ועוד.

2.7. **תווי שי** - המציע יספק מספר תווי שי בסכומים שונים הכרטיס יאפשר רכישת טובין ושירותים בפריסה ארצית במגוון בתי עסק כגון: רשתות מזון, הלבשה, הנעלה, מוצרי ספורט, מוצרים לבית , ספרים, תרבות. הכרטיס יאפשר רכישה בבתי העסק השונים גם במבצעים בערכו המלא.

2.8. **שוברים נוספים**- במידה וברשותו של המציע הזוכה שוברים נוספים מסוגים שונים, יורשה המתאם מטעם הרכבת לרכוש אותם בהתאם לתמחור האמור הנספח התמורה ובמסמכי פנייה זו.

2.9. תמהיל השוברים המבוקש יקבע על ידי המתאם ו/או על ידי נציגיו, שיוגדרו על ידו, ואין בכוונת הרכבת להתחייב לכמות שוברים או לתמהי רכישת השוברים.

3. **<u>תוקף השובר</u>**

3.1. השוברים יעמדו בתוקפם, לכל הפחות, למשך 24 חודשים ממועד מסירתם למתאם.

3.2. במידה ולא נוצל השובר במהלך תקופת התוקף בסעיף 3.2 לעיל, המציע הזוכה יאריך את השובר ב- 12 חודשים נוספים מתום התקופה הראשונה.

4. **<u>שירות</u>**

4.1. המציע הזוכה יהא בעל מערכת/אתר לניהול תקציבים לפי מחלקות ואליה תתאפשר גישה של מורשים מטעם הרכבת.

4.2. המציע הזוכה יהא בעל מערכת/אתר לניהול השוברים ובמידה והרכבת תחליט להעניק לעובדים בחירת שובר ליום הולדת או לכל אירוע אחר (חוויית יום הולדת) יוכל העובד לבחור שובר מבין מבחר שוברים שיוצעו לבחירה ויבחרו על ידי הרכבת ובהתאם לתקציב שיוקצה על ידה.

4.3. המציע יקים סביבה נפרדת באתר המתנות, בו יוצג מגוון השוברים כשהמחיר הנקוב יהיה המחיר לאחר הנחת המכרז. אל סביבת השוברים יוכלו העובדים להגיע גם באמצעות קישור (כתובת URL) ישיר.

5. **<u>הפעלת אתר אינטרנט לבחירת שוברים (חנות מקוונת)</u>**

5.1. על הספק הזוכה להפעיל אתר אינטרנט לבחירת שוברים, שיהיה נגיש לעובדי הרכבת/ נציגי הרכבת שיוגדרו לצורך בחירה.

5.2. פיתוח רספונסיבי - ממשק המשתמש יהיה מותאם לגודל ורזולוציית המסך בו המשתמש עובד. על האתר להיות רספונסיבי ומותאם לתצוגה במגוון מכשירים (מחשב / טבלאט / סמארטפון וכו').

5.3. הספק הזוכה יתחזק את האתר באופן שוטף, לרבות:

5.3.1. שמירה על נראות אחידה וייצוגית של האתר ונוחות המשתמש

5.3.2. תיקון תקלות טכניות ו"באגים" במערכת.

5.3.3. שמירה על פעולה רציפה ותקינה של האתר.

5.4. האתר יציע שוברים לעובדים על פי הקטגוריות ודרישת הרכבת כמפורט בסעיף 2 לעיל.

5.5. עובד הרכבת/נציג הרכבת שיוגדר מראש ייכנס לאתר באמצעות שם משתמש (מס' עובד) וסיסמא.

5.6. ניהול הרשאות – עובד יוכל לבחור שובר לרכישה ו/או שובר כמתנה באירוע אישי, בהתאם לדרישת המתאם. מנהלי מערכת יוכלו להעניק שוברים והוקרות לעובדים ולהנפיק דו"חות שימוש חטיבתיים. למנהל המערכת הראשית (מנהלת הרווחה או מי מטעמה) תהיה האפשרות להוסיף הרשאות ולהנפיק דו"חות מתקדמים לשימוש במערכת.

5.7. באחריות הספק הזוכה לבצע מעקב ובקרה על ביצוע ההזמנות באתר.

5.8. באתר תינתן אופציה לניהול תקציב (לדוגמא תקציב מחלקתי או יחידתי להזמנת שוברים).

5.9. במידה ויידרש קובץ זכאים הרכבת תעביר את הקובץ בהתאם לדרישות המערכת והפרמטרים שיוגדרו מראש לאתר הבחירה (לדוגמא אתר לבחירת שוברים לחוויית ימי הולדת).

6. **<u>הפעלת מוקד שירות לקוחות</u>**

6.1. על המציע הזוכה לספק מספר טלפון של שירות לקוחות, בו העובד יוכל לברר פרטים נוספים אודות השובר

6.2. הפעלת מוקד שירות לקוחות- הספק יפעיל מוקד שירות לקוחות למתן שירות לעובדי הרכבת/נציגי הרכבת גם במהלך בחירת שובר וגם לאחריה . מוקד השירות יפעל בימים א'-ה' בין השעות 00:16-00:09 לפחות

7. מתן הרשאת מנהל (ADMIN) לנציג הרכבת לקבלת מידע וסטטוס הזמנות בזמן אמת.

8. על גבי השובר תצוין באופן קריא רשימת החלופות אשר ניתן לממש באמצעות שובר הקנייה ו/או הפנייה לכתובת אינטרנט שבה מפורטת רשימת החלופות למימוש.

9. **<u>עיצוב והנפקת השובר</u>**

9.1. השוברים יונפקו על ידי המציע הזוכה ויימסרו למתאם מטעם הרכבת לאחד ממתחמי הרכבת בפריסה ארצית ו/או יישלחו לכתובת הדוא"ל של העובד ו/או לטלפון הנייד של העובד, והכל על פי בקשת המתאם ועל פי שיקול דעתו הבלעדי.

9.2. השוברים יחולקו לעובדים הזכאים על ידי הרכבת על ידי המתאם ו/או אחד מנציגי הרכבת.

10. **<u>SLA</u>**

המציע הזוכה יספק למתאם מטעם הרכבת את השוברים באופן מרוכז תוך 7 ימים קלנדריים מיום ביצוע הזמנה מהמתאם ו/או ממורשה הגישה למערכת מטעם הרכבת.

11. **<u>מימוש השובר</u>**

לשם מימוש הכרטיס ייגש העובד בצורה עצמאית לאחד מבתי העסק הקיימים באופציות הבחירה ועם הצגת השובר יקבל את השירות האמור בקריטריונים.

13. **<u>פיצויים מוסכמים – סל 2</u>**

13.1. במידה והספק הזוכה לא יעמוד באיכות השירות וברמות השירות המוגדרות, ייגבו ממנו פיצויים מוסכמים כמופיע בקנסות בגין אי עמידה בתקני שירות.

13.2. **מנגנון קנסות בגין אי עמידה בתקני שירות**

רמת שירות נדרשת	החריגה	גובה וסוג הפיצוי
תפעול תקין של אתר האינטרנט	תקלה טכנית הפוגעת ביכולת העובדים בשימוש באתר	קנס של 1,000 ₪ בגין כל יום בו התקלה לא מטופלת

נספח א'1

נספח סייבר לענן

גרסה: 1.2 תאריך: 28/04/2019

מסמך הנחיות עבודה - מחשוב בענן רכבת ישראל

1. כללי

1.1 מסמך זה מהווה נספח מחשוב ענן בהתקשרות מכרזית עם ממשקים עסקיים, וכן מעטפת הנחיות למערכות ענן בכל שלבי מחזור חייהם.

1.2 נספח זה ישמש כבסיס ומסגרת לפיהם תחליט יח' הסייבר מהם הסעיפים הרלוונטיים לנכס הסייבר הספציפי שנדון (תוך גריעה והוספה של הנחיות פרטניות לנושא).

1.3 מטרת נספח זה הינה לקבוע הנחיות עבודה אבטחת המידע בניהול\תחזוקה\תפעול מערכות מחשוב ונכסים של רכבת ישראל אשר יתקיימו בענן מחשובי.

1.4 מסמך זה קובע דרישות הן עבור רכבת ישראל והן עבור ספק אשר יבחר להעניק שירותי מחשוב בענן לרכבת ישראל.

1.5 מסמך זה הינו מסמך הרחבה לנוהל: 03-03-18 "שרשרת אספקה: נוהל אב".

2. הגדרות

2.1 הגדרות כלליות

ראה סעיף מס' 2 ("הגדרות"), בנוהל "שרשת אספקה: נוהל אב"/ "נספח שרשרת אספקה: נוהל אב".

2.2 הגדרות ייחודיות למחשוב בענן

שירותי מחשוב בענן הינם שירותי מחשוב הניתנים למשתמש באמצעות מחשב מרוחק, אליו מתחבר המשתמש דרך רשת האינטרנט או באמצעות קו תקשורת ייעודי.

הביטוי "ענן" הוא דימוי לרשת האינטרנט המבוסס על הצורה הגרפית בה מתארים את הרשת. הענן הינו מעין מסך הערפל שמושם בינינו לבין הטכנולוגיה והלוגיסטיקה, כאשר עיקר מעייניו הוא השירות שאנו מצפים לקבל מהענן.

בענן המחשוב נמצאים הנתונים והלוגיקה העסקית של מערכות המחשוב, בשרתים ובמרכזי מחשבים, והינם מופעלים מיחידות קצה מרוחקות.

כתוצאה מכך אין המשתמשים צריכים לרכוש ולנהל משאבים ומערכות מחשוב ובמקום זאת הם שוכרים אותם כשירות מספקים אשר מעמידים כוח מחשוב שהגישה שלו הינה דרך אינטרנט.

ענן המחשוב מאפשר למשתמש\ארגון שליטה וויסות של עוצמת המחשוב הנדרשת.

2.3 סוגי שירותים עיקריים במחשוב ענן

2.2.1 תוכנה כשירות - Saas - Software as a Service

במקרה זה המשתמש משתמש גם בתשתית חומרה, גם בפלטפורמה וגם בשירותים אפליקטיביים שפותחו על ידי הספק. במקרים רבים השירותים המסופקים בשיטת Saas הם שירותים בתפיסת SOA - (Service Oriented Architecture).

2.2.2 פלטפורמה כשירות - PaaS - Platform as a Service

השירות הניתן במקרה זה הוא פלטפורמה הנדרשת להרצה, הפעלה או פיתוח יישומים ע"י הלקוח. מדובר הן ביישומי מדף והן בפיתוח אפליקציות של המשתמש. במקרה זה, מקבל המשתמש גם משאבי מחשוב וגם תוכנות תשתית הנדרשות לצורך הרצת המערכת או פיתוחה. זאת, מבלי לדאוג לתחזוקה של מערכת ההפעלה, חומרת השרתים, איזון עומסים או קיבולת מחשוב.

2.2.3 תשתית כשירות - Iaas - Infrastructure as a Service

שירותים מסוג זה הם שירותים בהם המשתמש מקבל משאבי מחשוב לשימושו: שרתים, אחסון, שולחן עבודה או רשת.

2.2.4 שולחן עבודה כשירות - DaaS - Desktop as a Service

במודל זה הלקוח מקבל סביבת עבודה מלאה בה הוא יכול להפעיל את השירותים הנדרשים כאילו הוא עובד מול מחשב אישי כאשר המשאבים והיישומים נמצאים בחלקים אחרים של הענן או בעננים אחרים.

2.2.5 רשת כשירות - Naas - Network-as-a-Service

במודל זה הלקוח מקבל שירותי רשת על בסיס מנוי או תשלום ע"פ צריכה.

2.2.6 אבטחת מידע כשירות - SECaaS - Security as a Service

במודל זה הלקוח מקבל שירותי אבטחת מידע על בסיס מנוי או תשלום ע"פ צריכה.

2.2.7 "**ספק מחשוב ענן**" (Cloud Provider): חברה המספקת תשתית, פלטפורמה, תוכנה, או אחסון כשירות מחשוב ענן.

2.2.8 תצורות הטמעת מחשוב ענן:

2.2.8.1 "**ענן פרטי**" (Private Cloud): שירות המוצע על גבי רשת האינטרנט, או בתוך רשת פרטית. שירות זה הינו סביבה מבודדת וייעודית לארגון אשר ממוקמת בסביבת מחשוב ענן ואינו חשוף לציבור הרחב.

2.2.8.2 "**ענן ציבורי**" (Public Cloud): שירות המוצע על גבי רשת האינטרנט. שירות זה חשוף לציבור הרחב והינו חיצוני לתשתיות הארגון.

2.2.8.3 "**ענן היברידי**" (Hybrid Cloud): שילוב של ענן פרטי וענן ציבורי, אשר פועלים באופן עצמאי אחד מהשני, ומאוחדים ע"י תוכנה ותהליכים אשר מאפשרים שינוע מידע ויישומים.

3. חוקי המדינה ו/או רגולציה מחייבת

3.1 מערכת המחשוב בענן של הספק תמלא מלואן את כל ההוראות והחוקים במדינת ישראל ו/או כל רגולציה מחייבת, **דוגמת:**

3.1.1 חוק המחשבים.

3.1.2 חוק הגנת הפרטיות ותקנות העזר, ובכלל זה הנחיות הרשות להגנת

פרטיות. (ראה סעיף 7.6)

3.1.3 חוקי דיני ראיות.

3.1.4 כל חיקוק עתידי לניהול מאגרי מידע ולשמירתם.

3.1.5 איסוף ראיות דיגיטליות וזימון עובדי הספק לעדות, אם הדבר יידרש

3.1.6 ממשקים בין הספק לבין מערכות ר״י.

3.2 חוקיות התוכנה ופלטפורמת מחשוב

3.2.1 הספק יצהיר שכל התוכנות ומערכות המחשוב אשר משמשים אותו למתן השירותים לר״י הינם חוקיים, ונמצאים בבעלותו הבלעדית.

3.3 פירוט רגולציות ותקנים נוספים

3.3.1 על הספק להכיר ולציין (ככל שרלוונטי לשרות הניתן ורגישות המידע) האם פתרון הענן המוצע על ידו עומד ברגולציות ותקנים, **כגון:**

3.3.1.1. ISO 27001 ונגזרותיו.

3.3.1.2. ISO/IEC 27036:2013 - שרשרת אספקה.

3.3.1.3. PCI DSS

3.3.1.4. Nist (National Istitute for Standards and Technology)

3.3.1.5. Csa(cloud security alliance) – ver. 4

3.3.1.6. (Federal Risk and Authorization Management Program) Fedramp.

3.3.1.7. תקני ITU-T X.

3.3.1.8. תקנים ופרקטיקות לניטור וחיווי

3.3.1.9. תקנים אשר תומכים בהסדרת נושא דיווח אירועים, כגון: SSAE-18 ו - ISAE 3402.

3.3.1.10. תקנים בינלאומיים לניהול תשתיות מחשוב.

3.4 זכויות רכבת ישראל לנגישות למידע

3.4.1 ליח׳ הסייבר זכות לדרוש מהספק לפרט את המסלול הגיאוגרפי שהמידע עובר.

3.4.2 ליח׳ הסייבר הזכות לבצע בדיקות נאותות (Due Diligence) עיתיות אצל הספק הענן, בהתאם לשיקול דעתה וככל שישים ורלוונטי.

3.4.3 לדרוש מהספק לספק גישה מלאה לנתוני המידע המאוחסן.

3.4.4 הספק יספק לר״י אפשרות לתחקור המידע ללא עלות תפעולית ויעמיד לרשותה רוחב פס תואם לצורכי איסוף מידע-Forensic.

3.4.5 הספק יאפשר לר״י במקרה הצורך לגשת למידע ולאספו.

3.4.6 מידע המועבר לר״י יועבר בשיטות ובפרוטוקולים ופורמטים מקובלים, הניתנים לפענוח על ידי ר״י, ולא בפרוטוקולים יעודיים (Propriety).

3.4.7 הספק יאפשר לר״י בהינתן הצורך לבצע שימוש משפטי במידע הנמצא בענן.

4. נהלים

4.1 הספק יפרט אודות נהלי הסייבר ואבטחת המידע ברשותו ואשר בהם עושה שימוש, כגון:

4.1.1 אבטחת נכסי מידע של הלקוח.

4.1.2 אבטחת יישומים של הלקוח.

4.1.3 ניהול הרשאות

4.1.4 שרידות, גיבוי, המשכיות עסקית.

4.1.5 אבטחה פיזית ולוגית.

4.1.6 אבטחת רשתות.

4.1.7 אירועי אבטחת מידע, ניהול תגובה, תחקור וכו'.

4.1.8 פיתוח ותחזוקה של המערכות.

4.1.9 ביקורות.

4.1.10 הגנת פרטיות.

4.1.11 ניטור וחיווי.

4.1.12 נהלי טיפול משאבי אנוש וניהול מחזור חיי עובדים(קבלה, עזיבה וכו')

4.1.13 תוכנית מודעות עובדים.

4.2 הספק יציין האם הוא נוהג לתקף את הנהלים אחת לשנה, ומתי תוקפו לאחרונה הנהלים אותם

4.2.1 הספק יעביר לרשות ר"י העתק נהלים אשר ברשותו ואשר עסוקים בנושאי אבטחת מידע הגנת הפרטיות.

5. ניתוח וניהול סיכונים

5.1 מנהל המערכת/יזם ינתח את סיכוני הטמעת הנכסים הארגונים בענן.

5.2 הנכס יחולק ל 2 חלקים עיקריים:

5.2.1 נתונים (כגון: מה רמת רגישותם, למה משמשים וכו')

5.2.2 אפליקציות\תהליכים (כגון: מה התהליך שנדרש לבצע בנתונים)

5.3 בהתאם לשיקול דעתה של יח' הסייבר יופנה הספק למילוי פרק "ענן" בשאלון "**גרסה 1.1 של שאלון הספקים לחיזוק שרשרת האספקה**", שפורסם ע"י מערך הסייבר הלאומי.

6. מיפוי זרימת נתונים

6.1 בטרם ההטמעה נדרש מיפוי זרימת הנתונים בין כלל שירותי הענן לבין מערכות מחשוב הפנימיות ברכבת וכל לקוחות / צמתים אחרים. לפני קבלת החלטות יבין יש להבין לעומק את תצורת זרימת מידע אל\מ שירותי ענן.

6.2 באחריות היזם / מנהל המערכת בענן כי המיפוי הנ"ל יתבצע על ידי הספק על כל ישלח לאישור טרם הטמעתו ליחידת הסייבר .

6.3 המיפוי יעודכן בכל תוספת של מערכת/ יישום וכו'.

7. ארכיטקטורת מערכות ספק ענן

7.1 ארכיטקטורת מערכות ספק ענן תאופיין על ידי הספק בהתבסס על צרכי ר"י ובהתאם לנכסיה.

7.2 באחריות היזם / מנהל המערכת בענן כי אפיון הארכיטקטורה יובא לאישור יחידת הסייבר טרם הטמעתו .

8. ממשקים למערכות ספק הענן

8.1 מערכות הספק

8.1.1 הספק ימפה את ערוצי התקשורת למערכותיו הן בטווח הפנימי (גישה בין מערכות הספק) והן בטווח החיצוני (גישה מבחוץ למערכות הספק) .

8.1.2 הספק יישם מנגנוני אבטחת המידע והסייבר שיבטיחו את זהות ערוצי תקשורת אלה כשייכים לארגון.

8.1.3 הספק יישם מנגנוני אבטחת מידע והסייבר שיבטיחו הגנה מרבית על מערכות מערוצי תקשורת אלה .

8.1.4 תוגדר פעילות לאיתור ניסיונות התחזות דרך ערוצי תקשורת אלה.

8.1.5 הספק יידע את יח' הסייבר ברכבת ישראל בדבר הסיכונים הכרוכים בשימוש בערוצי התקשורת הנ"ל, למיטב הבנתו וידיעתו.

9. סקרי סיכוני אבטחת מידע ומבחני חדירה מבוקרים

9.1 יחידת הסייבר תיזום סקרי אבטחת מידע וסייבר בהתאם לשיקול דעתה, (וככל שישים), אשר עשויים לכלול בין היתר:

9.1.1 יישום אבטחת ארכיטקטורה בענן בכל הקשור לנכסי רכבת ישראל.

9.1.2 ממשקים בין מערכות ר"י לבין מערכות הספק.

9.1.3 נושאים נוספים אשר למשנתה מחייבים התייחסות.

9.2 הסקרים עשויים לבחון את נושאי הניהול, את יעילות אמצעי ההגנה שיושמו בפלטפורמה של הספק, ואת רמת הגדרות אבטחת המידע במערכות המידע, הן ברמת התשתית והן ברמת האפליקציה.

9.3 יחידת הסייבר עשויה ליזום מבדקי חדירה (Penetration Tests) הן ברמת התשתית והן ברמת היישום (אפליקציה), המדמים ניסיונות פריצה ע"י פורצים מתוך ומחוץ לארגון, הן כמשתמש קיים והן כפורץ ללא חשבון קיים. תדירות מבחני החדירה תיקח בחשבון את רגישות המערכת בהתאם.

10. מסירת מידע לצד ג' והסכם חסיון

10.1 הספק לא ימסור מידע ממאגרי המידע, ומידע על אבטחת המערכות נשוא ההתקשרות זו (ו-או כל פרויקט אחר המנוהל עבור רכבת ישראל) לשום גוף או אדם, ללא אישור בכתב של

יחידת הסייבר, ו/או יתר הגורמים הרלוונטיים ברכבת (כגון אגף בטחון, המחלקה המשפטית, מנהל המערכת וכו'), בהתאם להחלטות שיתקבלו לאחר הגשת בקשה למסיר מידע.

10.2 אף אם הספק יקבל צו שיפוטי המתיר לגורם ממשל ו\או גורם צד שלישי לגשת למידע, הספק יתחייב לאפשר לרכבת ישראל להגיש התנגדות לצו, וזאת לפני מסירת המידע לגורם הממשל ו\או גורם צד שלישי.

10.3 הספק יערוך ויקיים נוהל רישום מסודר של העברה\קבלה מידע כלשהוא בנוגע לנכסי רכבת ישראל לגורם מוסר\מקבל מידע, תוך רישום פרטי המקבל\מוסר, סוגי רשומות ומועדי מסירה וקבלה, רישום הנ"ל יועבר מדי חצי שנה ליחידת הסייבר.

11. ניהול מידע וזליגת מידע

11.1 הספק יישם תצורת אחסון אשר תיישם הפרדה וסגמנטציה בין לקוחותיו ובתוך ארגונו עצמו.

11.2 הספק יגן על המידע בכל אחד משלבי חייו (כניסה לענן, מעבר בין סביבות ענן שונות, ויציאה לגורם חיצוני).

11.3 הספק יטמיע אמצעי ניטור כגון DAM-Database Activity Monitoring ו FAM-File Activity Monitoring.

11.4 הספק יישם ויפרט מהם מנגנוני הבטחת ההגנה ומניעת זליגת המידע בהם הוא עושה שימוש על מנת:

11.4.1.1. למנוע זליגת מידע בין לקוחותיו.

11.4.1.2. למנוע זליגת מידע לא מאושר ממערוכותיו לטווח הציבורי.

11.4.1.3. למנוע זליגת מידע ע"י עובדי הספק.

11.4.1.4. לנהל את בעלי הרשאות מטעמו.

11.4.2 הספק יפרט מהם מערכות הניטור אשר ברשותו, וכיצד מנוהלים תוצריהן.

11.4.3 הספק ידווח מידי ליח' הסייבר במידה והתרחש אירוע (או חשד לארוע) של זליגת מידע מנכסי רכבת ישראל.

12. שינויים וניוד

12.1 פתרון הספק יושתת על API (מלא) סטנדרטי ומוכר למקרים בהם הרכבת תרצה לנייד את שרות הענן לספק אחר (על מנת להקל על המעבר משרות לשרות)

12.2 הספק ישתמש במערכות מוכרות להפעלת הסביבה הווירטואלית (כגון-Microsoft Hyper V server, VMWARE ESX, וכו').

12.3 הספק יספק קבצי קונפיגורציה בעת מעבר לספק אחר, או בעת בקשה מעת יח' הסייבר.

12.4 דרישות פרטניות לתצורות שונות:

12.4.1 IAAS:

12.4.2 הספק יידרש לבצע שימוש בפורמטים ידועים של VM (כגון VMDK, OVF, OVA, VHD, VHI וכו')

12.4.3 תוספות ייעודית למער הווירטואליזציה ינוהל תזוהה ותתועד. (בין היתר: יאושר תחילה, ויתועד לצורך זיהוי).

12.4.4 PAAS:

12.4.4.1. הספק יבסס את מערך הענן על עקרונות וטכנולוגיות מוכרות ומקובלות (כגון API), לטובת מעבר חלק בין הספקים.

12.4.4.2. הספק יידרש כי הארכיטקטורה תאפשר את ניתוק המידע מתשתית הספק באופן פשוט ותוך שמירה על שלמות , חסיון וזמינות המידע.

12.4.5 SAAS:

12.4.5.1. הספק יעמוד בדרישה כי ניתן יהיה להמיר את המידע למידע שמיש ללא תלות באפליקציה קניינית (Proprietary), או תלות אחרת בספק.

13. אבטחת מידע

13.1 אבטחה פיזית וסביבתית (בהיבט סייבר)

13.1.1 אגף בטחון ברכבת ישראל הוא הגורם הבלעדי המנחה בהתייחס לאבטחה הפיזית (לרבות הנחיות בהתייחס לספקים הנדרשים לסיווג בטחוני).
הסעיפים הבאים מפרטים דרישות סף לספקי ענן, ואינם מהווים תחליף לדרישות אגף בטחון ברכבת ישראל, ככל שאלה יועברו.

13.1.2 הספק יחלק את סביבת העבודה למעגלי אבטחה/אזורים מאובטחים לפי רמות רגישות.

13.1.3 הספק יישם מדיניות של מספר מעגלים של בקרות גישה פיזית.

13.1.4 נכסי רכבת ישראל ישמרו\יעובדו\יגובו באזורים אשר ניתן להם סיווג נכסים בעלי מידע עם רגישות גבוהה.

13.1.5 הספק יישם מערכת אבטחה משולבת באמצעים טכנולוגיים כגון מצלמות, קוראי כרטיסים, אמצעים ביומטריים, ואמצעי התראה מסורתיים, כגון מנעולים ומפתחות.

13.1.6 אמצעי בקרה תפעוליים ישולבו לצורך ניטור אוטומטי ומתן התראה במקרה ומתרחשת פריצה או בעיה.

13.1.7 ניהול גישה לנכסים פיזיים יבוצע באופן מרכזי אשר ישלב רשומות הניתנות לביקורת באמצעות ריכוז זרימת העבודה עבור תהליכים לבקשה, לאישור למתן גישה למרכזי נתונים

13.1.8 ניהול גישה זה יפעל על פי עיקרון של מתן גישה מינימלית נדרשת (Least Privilege) וישלב תהליכי זרימת עבודה להשגת אישורים מגורמי אישור מרובים.

13.1.9 יבוצע תיעוד ודיווח בבקרת מרכז נתונים ראשי והעתק התיעוד והדיווח יומצא לרכבת ישראל, בעת דרישה.

13.1.10 גישה פיזית של אנשי הספק לנתוני רכבת ישראל תידרש לשילוב של מספר גורמים לאימות (Multi factor authentication – כגון קורא כרטיסים על מנת להיכנס לחדר, ושימוש בסיסמא/ות על מנת להתחבר ולגשת למידע).

13.1.11 כל ניסיון גישה פיזי חריג ושאינו בהתאם להרשאות אשר הוסכמו ואינו על פי אימות כנדרש, יתוחקר וידווח ליח' הסייבר (ו/או לאגף בטחון בהתאם לדרישתו) בהקדם.

13.1.12 הוצאת ציוד המכיל מידע \ נכסי רכבת ישראל מאחד ממעגלי האזורים המאובטחים תתבצע תוך ידוע ואישור מקדמי של מנהל המערכת ויח' הסייבר.

13.2 **אבטחת וניהול רשתות**

באחריות הספק:

13.2.1 ליישם רבדים של אבטחה בין רשתות שונות של לקוחותיו.

13.2.2 ההפרדה הרשתות תתאפיין הן במישור הניהולי, והן במישוריים התפעוליים והבקרתיים.

13.2.3 ליישם ולפרט את ההפרדה הרשתית אותה מיישם, בהתייחס לפרויקט המנוהל בענן.

13.2.4 ליישם ולפרט אודות המערכות בהן עושה שימוש למניעה\בקרה\פיקוח על תקלות\התקפות\שיבוש בין רשתות השונות של הספק, לרבות ההתממשקות לרשת רכבת ישראל (ככל שישנה).

13.2.5 ליישם ולפרט אודות מערכות ההגנה אשר מגנות באופן הולם על מערכות המחשוב, הנתונים, מהימנות הנתונים וזמינות הנתונים.

13.2.6 ליישם ולפרט אודות מנגנוני מניעה ובקרה לזליגת מידע בין רשתות שונות.

13.2.7 לפרט אודות מערכות בקרה של הספק אשר מתריעות על כל חריגה מהמוזכר בסעיפי 13.2.

13.3 **אכיפת בקרות גישה וניהול הרשאות**

13.3.1 יישמו מנגנונים ממוכנים לניהול בקרות גישה למערך הענן.

13.3.2 בקרות גישה יורכבו מאמצעי זיהוי, אימות, ובקרת הנתיב.

13.3.3 ההרשאות יינתנו בהתאם לעקרונות הנדרש לביצוע התפקיד (least privilege), ובהתאם לצורך לדעת (need to know).

13.3.4 מדיניות בקרת גישה תיקח בחשבון מידור מתאים של הרשאות.

13.3.5 הספק יעביר ליח' הסייבר (ו/או לאגף בטחון בהתאם לדרישתו, ורמת סיווג המערכת), פרטים מלאים של בעלי תפקידים אשר להם הרשאות לנכסי רכבת

13.3.6 מתן הרשאות גישה למערכות ושירותים יוגדרו ויבוקרו בהתאם לדרישות נוהל רכבת ישראל "ניהול משתמשים וזהויות" (01-08-18)

13.2.2 הגישה לשירות הענן מרשת מהאינטרנט לא תאופשר ללא אישור מפורש של יח' הסייבר.

13.4 **אמצעי זיהוי ואימות**

13.4.1 ייקבעו אמצעי זיהוי למערכות ושירותים לצורך זיהוי חד ערכי (Unique User ID) של המשתמש.

13.4.2 אמצעי הזיהוי יהיו אישיים ולא יותר שיתוף של אמצעי זיהוי אלה.

13.4.3 אמצעי הזיהוי יוחלו הן על מנהל מערכת ברכבת ישראל והן על כלל המשתמשים אחרים (ספקים וכדומה) המתחברים למערכות המחשוב בענן.

13.4.4 לכל הפחות, אמצעי הזיהוי יורכבו משילוב של שם משתמש וסיסמא, תוך העדפת זיהוי - אימות מרובה אלמנטים (Multi factor authentication), ככל הניתן, ובהתאם לרגישות המידע כפי שיוגדר בפרויקט.

13.4.5 נתוני הזיהוי והאימות יישמרו ויועברו באופן חסוי (הן בתווך התקשורת והן במערכות השונות).

13.4.6 יח' הסייבר תשקול שימוש באמצעי זיהוי חזק ושימוש בטכנולוגיה המונעת אפשרות העתקה או שחזור הפריטים, בהתאם לשיקול דעתה, ורגישות המידע כפי שהוגדר בפרויקט.

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

13.5 **ניהול סיסמאות משתמשי הענן**

13.5.1 ניהול הסיסמאות (לרבות מורכבות, החלפה וכו') יתבצע בהתאם לדרישות נוהל רכבת ישראל "אמצעי הזדהות וסיסמאות (02-08-18)".

13.5.2 על מנגנון ההגנה לכלול הגנה מפני מתקפות Brute (כגון נעילה אחרי מס' ניסיונות, מתן הודעה כללית – ללא ציון אם מדובר בזיהוי או אימות שגוי" וכו')

13.5.3 סיסמא תבוטל מידית בכל מקרה של חשש לפגיעה בחשאיותה, ולא יתאפשר לשחזר את הסיסמא.

13.5.4 סיסמאות לא ישמרו במצבם הטקסטואלי (Plain text), אלא בהצפנה בלבד, רצוי בתוספת ערך רנדומלי כלשהו (Salt) אשר יקשה בפיצוחן.

13.5.5 דליפת סיסמא/ שימוש לא מורשה/ניסיון לשימוש לא מורשה בסיסמא ידווח ליח' הסייבר במידי.

13.6 **ניטור, לוגים ובקרה**

13.6.1 קבצי החיווי (לוגים) יהיו זמינים לבחינת נציג רכבת ישראל על פי דרישה, וללא כל עלות/חיוב נוסף.

13.6.2 כל פעולה תתועד ברשומה אבטחתית ותשלח (במקרה הצורך וכפי שיוגדר ע"י יח' הסייבר), למרכז ניהול האירועים (SIEM) של רכבת ישראל.

13.6.3 המערכת תתמוך ביכולת העברת קבצי חיווי ל-SIEM בהתאם לסטנדרטים מקובלים, כגון Syslog.

13.6.4 הספק יפעיל מנגנון רישום פעולות ברמת מערכת ההפעלה בשרת השירות, לרישום כניסה ויציאה של חשבונות ניהול (Administrator), תמיכה, DBA, Audit System, משתמשי המערכת, וכו'.

13.6.5 הספק יפעיל מנגנון רישום, בקרה ודיווח להפקת דו"חות גישה לתשתיות התוכנה ולמסדי הנתונים (Data Bases). בנוסף, המערכת תאפשר למנהלי המערכת, בהתאם להרשאתם, להגדיר מהם הרכיבים אשר הפעילות בהם תתועד בקבצי החיווי.

13.6.6 להלן פעולות בקרה המהוות דרישות חובה ליישום במערכת, עבור ניטור, חיווי ובקרה:

13.6.6.1. הזדהות שגויה.

13.6.6.2. כל שינוי, או מחיקת אובייקטים במערכת.

13.6.6.3. כל שינוי (לרבות מחיקה) בתכנה, בטבלאות, בנתונים ובבקרות של מסדי הנתונים.

13.6.6.4. אירועים אפליקטיביים שיוגדרו כדורשי בקרה עפ"י מנגנון כללים מיוחד לנושא.

13.6.6.5. התחלת פעילות מסוימת אשר תוגדר כדורשת בקרה ע"י המשתמש (כגון: פתיחת כספת, שליחת מסר וכו').

13.6.6.6. ביצוע פעילויות המבוצעות על-ידי גורמים בעלי הרשאות גבוהות.

13.6.6.7. פעולות אדמיניסטרציה (ניהול משתמשים, הורדה והעלאת מערכת, services, וכו').

13.6.6.8. שגיאות תפעוליות (נפילת מערכת, הודעות שגיאות תוכנה, וכו').

13.6.6.9. הפקת דו"ח כשלים בהליכי הזדהות, או בניסיונות גישה בלתי חוקיים ברמת מערכת ההפעלה ומסד הנתונים.

13.6.7 עבור כל אירוע המוגדר כדורש בקרה, יישמרו הפרטים הבאים:

13.6.7.1. תאריך ושעה.

13.6.7.2. מקור ביצוע הפעולה (דוגמא: כתובת IP, domain)

13.6.7.3. שם המשתמש.

13.6.7.4. סוג האירוע.

13.6.7.5. הצלחה, או כישלון של האירוע.

13.6.7.6. זיהוי האובייקט עליו מבוצעת הפעולה (שם קובץ וכו').

13.6.7.7. תיאור הפעולה (מה בוצע?): עבור כל סוג אירוע יש לספק תוכן רלוונטי. למשל: עדכון רשומה, ניסיון גישה לרשומה, מחיקת משתמש, הורדת מערכת וכו'.

13.6.8 קבצי החיווי (לוג) במערכת יהיו מוגנים מפני גישה (צפייה, שינוי, מחיקה) לא מורשית ותישמר האפשרות לזהות גישה לא מורשית.
המערכת תתריע על ניסיון גישה/שימוש, החורג מגבולות ההרשאות שניתנו.

13.6.9 אבטחת רשומות: באחריות הספק ליישם מנגנוני בקרה בנושא זה ולוודא כי מידע אישי וכן רשומות המערכת לא ייחשפו בפני גורמים בלתי מורשים.

13.6.10 על המערכת לנהל תהליך מובנה וסדור של אחסון ומחיקת רשומות.

13.6.11 על ההודעות צריכות להיות אמינות, מלאות וברורות.

13.6.12 המציע יפרט אודות יכולת מנגנון הבקרה להתממשק למנגנון הדו"חות ולספק רמה גבוהה של דוחות, חיתוך מידע, וכו' .

13.6.13 על המציע לפרט אודות יכולות דיווח של המערכת (כגון: דוא"ל, SMS, וכו') למנהלי המערכת על אירועים שיוגדרו כדורשי דיווח.

13.6.14 על מערך הבקרה להיות מאובטח כיאות. רק משתמשים מורשים יקבלו גישה אליו, ובמיוחד יש להקפיד על בקרת גישה ליכולת להעלות ולהוריד את מנגנון הבקרה.

13.6.15 המידע אשר ישמר בקבצי החיווי יעמוד בדרישות תקן אבטחת מידע בסקטור כרטיסי האשראי (PCI-DSS) ובתקנות הרשות להגנת הפרטיות, ככל שרלוונטי לנושא.

14. הפרדת סביבות

14.1 הספק יציין אודות הפרדת סביבת הייצור של המערכת מסביבות אחרות כגון פיתוח ובדיקות.

14.2 כל גזירת מידע מ/אל סביבת הייצור מ/לסביבה אחרת תתבצע בתיאום עם יח' הסייבר ותוך וידוא כי הסביבה אליה נגזר המידע מאובטחת בהתאם לרגישות המידע המועבר.

14.3 יצוין כי בכל מקרה העברת מערכות ומידע מסביבות פיתוח לייצור יערכו בצורה מבוקרת, בהתאם לנהל רכבת ישראל "אפיון פיתוח" (01-09-18), בכדי למנוע פגיעה בנתונים בסביבת הייצור.

15. תהליך ניהול המידע של רכבת ישראל במערכות ספק המחשוב בענן

15.1 העברת המידע

בתהליך העברת מידע בתווך תקשורת ציבורי או על גבי מדיה ניידת, הספק יפרט אודות:

15.1.1 כיצד מוגן המידע, ובאילו אמצעים מקובלים לשמירת סודיות, אמינות ושלמות הנתונים נעשה שימוש.

15.1.2 באילו במנגנוני הצפנה נעשה שימוש על מנת להגן על המידע.

15.2 זמינות המידע

15.2.1 בהתאם לשיקול דעתו של מנהל הפרויקט/מנהל המערכת יוגדרו יעדי זמינות מידע בפרויקט. יח' הסייבר תעודכן אודות יעדים אלו.

15.2.2 הספק יפרט:

15.2.2.1. באילו כלים נעשה שימוש להבטחת זמינות הנתונים

.

15.2.2.2. מהם מגנוני הכפילות והיתירות של מערכות בהם נעשה שימוש, המערכות לחלוקת עומסים, הכלים לייצוב מתח חשמלי וכדומה.

15.3 גיבוי המידע

15.3.1 מנהל הפרויקט/מנהל המערכת יגדיר דרישות גיבוי למערכות המידע השונות בהתאם לרמת הרגישות שנקבעה בהערכת הסיכונים.

15.3.2 הספק יפרט אודות פעילות גיבוי המידע, לרבות מודל האחסון והגיבוי (כגון: גיבוי מלא, גיבוי מלא + גיבוי מצטבר, גיבוי מלא + גיבוי שינויים, ובאיזו תדירות, מה התרגולים שמבוצעים וכו').

15.3.3 יח' הסייבר תבקר את איכות הגיבויים (כולל שחזורים יזומים) אשר מבוצעים ידי הספק, בהתאם לשיקול דעתה.

15.3.4 על הספק לבצע שמירת אמצעי הגיבוי במקום מרוחק, מאובטח ומוגן בפני פגיעה באמצעים ובתוכנם.

15.3.5 בהתאם לשיקול דעתו של מנהל הפרויקט/מנהל המערכת תוגדר התדירות בה יועברו עותקי נתונים עדכניים של נכסי ר"י לאחסון בשרתי רכבת ישראל, ככל שנדרש. יח' הסייבר תעודכן אודות הגדרות אלו.

15.4 חסיון ושלמות המידע

15.4.1 הספק יפרט אודות מנגנוני הצפנה להגנה על חיסיון מידע\נכסי הסייבר האגור באמצעי האחסון שבאחריותו.

15.4.2 הספק יפרט אודות מנגנוני ההצפנה בהם נעשה שימוש להתקשרות וממשק בין מערכות הרכבת למערכות המחשוב בשרות הענן אותו הוא מספק.

15.4.3 ככל שיידרש, ובהתאם לרגישות המידע כפי שהוגדר ע"י מנהל הפרויקט/מנהל המערכת, פתרון הספק צריך לתמוך בין היתר ב :

15.4.3.1. הצפנת כלל המידע הרגיש אשר עולה לענן.

15.4.3.2. יכולת הצפנה ברמת האפליקציה (PAAS).

15.4.3.3. מפתחות ההצפנה ישמרו מחוץ לאפליקציה ולא אצל הספק.

15.4.3.4. יש לקיים שימוש (אם אפשר) ב – HASH (מנגנון גיבוב) כך שרק ה- HASH ישמר בענן.

15.4.3.5. הצפנת לוגים ו- metadata ללא תלות בתדירות פתיחת קבצי המידע.

15.4.4 ביצוע ושימוש בשיטות הצפנה מוכרות ומקובלות (כגון צופן בלוקים סימטרי מסוג AES), ולהימנע מהצפנה קניינית.

15.4.5 תהליך ההצפנה יבוצע בצורה ממוכנת ללא התערבות ידי אדם.

15.5 **חתימה דיגיטלית (Digital Signature) ומנגנוני מניעת התכחשות (Non-Repudiation)**

15.5.1 מנהל הפרויקט/מנהל המערכת יגדיר האם נדרש יישום חתימה דיגיטלית (למניעת אי-התכחשות שליחה ושלמות המידע המעובר מהענן).

15.5.2 החתימה תיושם באופן שיאפשר לגופים מחוץ לספק הענן לזהות את בעלי החתימה הדיגיטלית באופן המקובל בסטנדרטים בין-לאומיים ובהתאם לחוק חתימה דיגיטלית.

15.5.3 הספק יציין מהם מנגנוני מניעת ההתכחשות בהם נעשה שימוש בפתרון כדי ליישב מחלוקות לגבי התרחשות או אי-התרחשות של אירועים או ביצוע פעולות.

16. **BCP - (Business Continuity Management)**

16.1 ספק מחשוב הענן יפרט את התכנית שברשותו אשר מתוכננת לתמוך בהמשך הפעילות העסקית עבור נכסי ומערכות השייכות לרכבת ישראל במצבי משבר Business Continuity Planning), אלא אם יגדיר מנהל הפרויקט/מנהל המערכת שאין צורך ב- BCP, אלא רק לגיבוי המידע.

16.2 באחריות היזם לדאוג להסכם/נספח SLA ייעודי אשר תפרט הגדרות אלו.

16.3 תכנית ה – BCP תתייחס בין היתר להיבטים הבאים:

16.3.1 קביעת התהליכים העסקיים הקריטיים שיש להפעילם במצבי משבר וחירום, תוך זמן סביר.

16.3.2 הקמת אתר חירום לצורך הפעלת מערך טכנולוגית המידע ופרק הזמן המרבי להפעלתו מרגע התרחשות האסון או ההכרזה על מצב חירום.

16.3.3 מעבר ויישום תוכנית התאוששות מאסון – Disaster Recovery Plan (DRP).

16.3.4 תרגול והפעלת סימולציות בנוגע למצבי חירום שונים.

16.3.5 קיום מעקב אחר ביצוע בפועל של תכנית ההערכות.

17. דוחות

17.1 הספק יציין באילו דוחות תומך הפתרון המוצע, ומה התדירות בה ניתן להפיק דוחות אלו. רשימת דוחות לדוג':

17.1.1 יומן חריגים. הספק, ימציא את יומן האירועים החריגים לנציגי רכבת ישראל, במועד העברת הדרישה.

17.1.2 יומן מסירת מידע.

17.1.3 יומן הכנסת מידע.

17.1.4 יומן התחברות מרחוק נציגי רכבת.

17.1.5 יומן שדרוגים ופיתוחים.

17.1.6 דוח הרשאות מורשות גישה.

17.1.7 דוח אירועי אבטחת מידע.

18. ניהול אירועי סייבר ואבטחת מידע

18.1 הספק יפרט את תכניות הפעולה שברשותו להתמודדות עם אירוע סייבר - אבטחת מידע, והגנת המידע של רכבת ישראל. תכנית זו תציין האם ברשותו צוות (ומה הרכבו) להתמודדות עם אירועים אלו. הפירו יתייחס בין היתר ל:

18.1.1 **הערכות** – מוכנות הספק לתגובתה מידית עם התרחשות אירוע.

18.1.2 **זיהוי-** איתור גורם להתרחשות האירוע, בין מדובר באירוע מכוון ובין לאו.

18.1.3 **בלימה-** ביצוע פעולות בלימה כדי למזער ולבלום התפשטות אירוע לסביבות אחרות ומזעור הסיכון.

18.1.4 **מיתון-** אספקת שירותים רלוונטיים לצמצום הסיכון, ולהישנות האירוע.

18.1.5 **שחזור-** ביצוע שיחזור השירות ואו מידע בהתאם לצורך.

18.1.6 **הפקת לקחים-** לאחר פתרון אירוע האבטחה, הערכה, תיעוד והפקת לקחים.

18.1.7 בכל התרחשות אירוע סייבר – אבטחת מידע יעביר הספק למנהל הפרויקט/מנהל המערכת, וכן ליח' הסייבר על פי דרישה, דוח מרכז המתייחס לכלל הנושאים האמורים בסעיפי 18.1.1

18.1.8 על פתרון הספק לתמוך ביכולת הפקת הדוח האמור בסעיף 18.1.2 באופן מיידי.

18.2 הספק יתחייב לשתף פעולה ככל שיידרש עם יח' הסייבר ו/או עם כל גורם אחר מטעם רכבת ישראל:

18.2.1 בכל אירוע סייבר - אבטחת מידע, או כאשר קיים חשד לאירוע כזה.

18.2.2 בכל הפרה או חשד להפרה של חוקים, תקנות או נהלי סייבר – אבטחת מידע.

18.2.3 בחקירת אירועים או חשדות, לחריגות אבטחה.

18.3 הספק יתחייב כי הוא ועובדיו ישתפו פעולה עם גורמי חוק וביטחון במדינת ישראל, ובכלל זה יתייצבו למתן עדות במועדים אשר רכבת ישראל ו\או גורמי החוק והביטחון במדינת ישראל יקבעו.

18.4 על הספק להבטיח כי הניטור המתבצע על ידו עונה על דרישות חוק דיני הראיות במלואן.

18.5 בכל מקרה, יפעל הספק באופן מיידי על מנת לטפל באירועים בעלי אופי פגיעה אפשרית בזמינות\אמינות\שרידות\הרשאות\חסיון נכסי רכבת ומערכותיה.

18.6 ככל שנודע לספק על קיומן של פגיעויות בנושא סייבר - אבטחת המידע ו/או הגנת הפרטיות (אף אם טרם בשלו לכלל אירוע), ידווחו אלו למנהל הפרויקט/מנהל המערכת וליח' הסייבר באופן מידי.

18.7 לאחר עד 48 שעות מסיום האירוע ימסור הספק ליח' הסייבר דוח המתעד את אירוע הסייבר - אבטחת המידע ואת הראיות שנאספו במהלכו ומתעד את הפעילות שבוצעה בנידון. הדוח יכלול תיעוד כגון שמירת קבצים רלוונטיים, צילומי מסך, ובכל מקרה פירוט מספק על מנת להסיק מה אופי האירוע, מתי זוהה לראשונה וכיצד טופל.

18.8 הספק יבצע הליך הפקת לקחים ויתווה תכנית לטיפול באירועים דומים בעתיד.

19. ניטור ונתיב בקרה (Audit Trail)

19.1 הספק יתחזק מנגנון ניטור לפעילות, אשר יאפשר מעקב אחר נתיב הבקרה, ביצוע פעולות ושאילתות.

19.2 תכולת נתיב הבקרה תכיל את הנתונים הרלוונטיים שיאפשרו לגלות ניסיונות גישה, פעולות לא מורשות וזיהוי מקורן. נתיב הבקרה יכלול מידע לכל הפחות על ניסיונות גישה של מורשים ולא מורשים, מוצלחים ולא מוצלחים, מהות הפעולה, מקור הגישה זמן הגישה, וכו'.

19.3 הספק יבצע בדיקות סדירות של דוחות החיווי והבקרה המתקבלים ממערכות הניטור והמחשוב של החברה.

19.4 במסגרת הבדיקות הסדירות תיבדק זמינות המערכת והמשאבים, כולל בדיקת קיבולת המערכת ומגמות השימוש תוך זיהוי "צווארי בקבוק" אפשריים העלולים להוות איום וסכנה בהיבטי סייבר - אבטחת המערכת והמידע.

19.5 פרק הזמן לשמירת קבצי התיעוד ייקבע בהתאם להגדרת מנהל הפרויקט/מנהל המערכת והנחיות יח' הסייבר.

19.6 קבצי פעילות הניטור (קבצי ה – Log) יאובטחו בפני מחיקה, שינוי או קריאה בלתי מורשים.

19.7 על שעון מנגנון הניטור להיות מסונכרן עם מקור שעון מדויק לצורך דיוק התיעוד.

19.8 הספק יחזיק ברישום של כל המשתמשים אשר קיבלו גישה דרך רשת ציבורית, ככל שקיימים ואושרו כאלה.

20. סיום ההתקשרות

עם סיום ההתקשרות:

20.1 הספק מתחייב להשמיד כל מידע השייך לרכבת ישראל המצוי ברשותו ואשר לא נמסר לרכבת מסיבה כלשהי.

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

20.3 בהתאם לרגישות המידע המעובד, או מאוחסן במערכת (על פי סיווג המידע אותו יגדיר מנהל המערכת, או בעל המידע שאגור במערכת), או בעקבות דרישות רכבת ישראל, יתחייב הספק כי הדיסקים הקשיחים אשר הכילו מידע של רכבת ישראל, ימחקו בהתאם להוראות תקן FIPS SP 800-88 - Guidelines for Media Sanitation, כאשר יש להתייחס לכל פריט מידע כ"מידע רגיש"

20.4 במקרה והספק נדרש להמשיך ולהחזיק פריטים כנ"ל, עליו לחתום על הצהרה בה הוא מתחייב להעביר כל מידע ורכיב הנוגע למערכות ועובדי רכבת ישראל, רק לגורם מורשה מטעם רכבת ישראל ולאחר קבלת אישור כתוב ממנהל הפרויקט ומיח' הסייבר.

נספח א'2

נספח אבטחת מידע לחוזה – ספק מערכת מחשב

1. מטרת המסמך

1.1. להוות נספח אבטחת מידע לחוזה עם ספק מערכת/ציוד מחשב לרכבת.

1.2. מסמך אשר יתייחס להיבטי אבטחת מידע אשר על הספק ליישמם בהתקשרות עם רכבת ישראל.

1.3. נספח אבטחת מידע זה יצורף למכרז, בהתאם לרכש תכולתו.

2. כללי

2.1. פעילותה התקינה של חברת רכבת ישראל מושפעת ותלויה מרמת שלמותו, אמינותו, עדכניותו, זמינותו, שרידותו ושמירת סודיות המידע/מערכות.

2.2. המידע, המערכות המנהלות אותו, האמצעים והציוד עליו הוא מושתת, מהווים נכס מרכזי וחיוני של החברה ויש להגן עליהם כעל משאבים אחרים בעלי ערך בחברה.

2.3. פגיעה במידע, במאגריו או במערכותיו, לרבות חשיפה, חבלה או שיבוש, עלולים לפגוע בפעילות החברה עד לרמת השבתתה המלאה. הנזקים עלולים לתת אותותיהם בהיבטים מסחריים, עסקיים, שיווקיים, תפעוליים, טכנולוגיים וכספיים, עלולים להוביל לפגיעה במוניטין ובתדמית החברה.

2.4. היות וברכבת ישראל מתקיימים מכרזים מסוגים שונים ,אין לראות נספח זה מכיל ומקיף את כלל המכרזים.

2.5. בהתאם לתכולת המכרז יוסף נספח אבטחת המידע שיותאם אליו.

3. הגדרות

3.1. **ר"י**-רכבת ישראל

3.2. **ספק** - חברה אשר מתמודדת במכרז ומספקת שירותים, טובין, יעוץ לרכבת ישראל.

3.3. **יועץ** - חברה המספקת שירותי יעוץ לר"י על ידי עובדיה או מי מטעמה.

3.4. **נכס ר"י** - מידע, אפליקציה, מערכות, ממשקים השייכים לר"י.

3.5. **המכרז** – מכרז לקבלת טובין ,שירותי יעוץ, אספקת ותחזוקת מערכות מחשוב בר"י .

3.6. **מידע** - כל מידע (Information), ידיעה, מסמך, תכתובת, תכנית, נתון, מודל, חוות דעת, מסקנה וכל דבר אחר כיו"ב הקשור ו/או הנוגע למתן השירותים, לרבות מידע הנוגע לצנעת הפרט של עובדי החברה ,בין בכתב ובין בע"פ ו/או בכל צורה או דרך של שימור ידיעות בצורה חשמלית ו/או אלקטרונית ו/או אופטית ו/או מגנטית ו/או אחרת, הקשורים ו/או הנוגעים למתן השירותים, אשר אינו מצוי בנחלת הכלל.

3.7. **סודות מקצועיים** - כל מידע אודות הרכבת אשר יגיע לידי היועץ או עובד מטעמו בקשר למתן השירותים, בין אם נתקבל במהלך מתן השירותים או לאחר מכן, לרבות ומבלי לפגוע בכלליות האמור לעיל: מידע אשר יימסר ע"י המזמין ו/או כל גורם אחר ו/או מי מטעמו.

3.8. **איום** – **Threat**: אפשרות פוטנציאלית לפגיעה בשלמות, זמינות או חשאיות המידע.

3.9. **אמצעי זיהוי**-אמצעי המספק פרטים לגבי זהותו של אדם או מערכת בעת ניסיון כניסה ואישור ביצוע פעולות מטעמם למערכת מידע.

3.10. **גניבת זהות**- ניסיון לגניבת זהות או מידע אישי ע"י התחזות לגורם רשמי המבקש מידע זה .

3.11. **הערכת סיכונים**-תהליך של הערכת רמת הסיכון של המערכות השונות בארגון. התהליך ממפה את האיומים השונים הנובעים מהפעילות במערכות השונות.

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

3.13. **זיהוי חד ערכי** - ערך ייחודי המזהה את מי שמתיימר להיות בעל אמצעי הזיהוי.

3.14. **חשיפה** – Vulnerability- חולשה במערכת העלולה להוביל להתממשות איום.

3.15. **לוג** – **Log** - קובץ התיעוד של נתיב בקרה.

3.16. **מידע רגיש** - מידע שר"י סיווגה כבעל סיווג הדורש אמצעי אבטחת מידע נאותים כדי שיהיה נגיש רק למורשים.

3.17. **מערכות מידע** - כלל הציוד הממוכן התומך בעיבוד והצגת מידע של ההחברה הכולל בין השאר: שרתים, מחשבים נייחים וניידים, ציוד תקשורת, ציוד אבטחת מידע ועוד.

3.18. **נתיב בקרה** - תיעוד פעולות המתבצעות במערכות מידע. קובץ התיעוד מקשר את הפעולה לנתונים נוספים כגון: שם מבצע הפעולה, המועד, הפעולה עצמה ועוד.

3.19. **רמו"ט** – רשות מידע וטכנולוגיה במשרד המשפטים, האחראית לנושא הגנת הפרטיות ורישום מאגרי מידע.

3.20. **סקר סיכונים** - סקר המאתר איומים/חשיפות ,הקשורות באבטחת מידע במערכות שונות, ומעריך את רמת הסיכון שלהם לרכבת ישראל .

4. התקשרות עם ספק

4.1. סוגיות משפטיות מול הספק

4.1.1. ר"י תפנה את הטיפול בנושא למחלקה המשפטית ברכבת.

4.2. חוקי המדינה

4.2.1. ספק השירותים/מערכת ימלא במלואן את ההוראות והחוקים במדינת ישראל כדוגמת:

4.2.2. חוק המחשבים.

4.2.3. חוק הגנת פרטיות ותקנות העזר, ובכלל זה הנחיות רמו"ט.

4.2.4. חוקי דיני ראיות.

4.2.5. כל חיקוק עתידי לניהול מאגרי מידע ולשמירתם.

4.2.6. הנחיות גופים מנחים את הרכבת.

4.2.7. כל בירור והתדיינות בסוגיות משפטיות יתקיים בבית המשפט בתל אביב, וזאת בהתאם לחוק הישראלי. למען הסר ספק, יאסר על הספק לעלות השגות בנושא סמכות משפטית ו/או סמכות דיונית מקומית.

4.2.8. הסעיפים הנ"ל יוכנסו בחוזה שיחתם בין רכבת ישראל לספק.

4.3. חוזה

4.3.1. הספק יתחייב שלא למסור/להעביר מידע אשר יימצאו במערכותיו והינו שייך לרכבת ישראל – ללא אישור בכתב ומראש מהרכבת.

4.3.2. הספק ידווח לרכבת ישראל במידה והיה אירוע אבטחת מידע ו/או אירוע הגנת פרטיות ממערכותיו באופן מידי, אף אם למשנת הספק לא נגרם נזק ו/או חשיפה כתוצאה מהאירוע הנ"ל.

4.3.3. החוזה ינוסח בצורה אשר תחייב לנקוט בכל הצעדים הנדרשים לשם הגנה על המידע.

4.3.4. בחוזה ייקבעו בין השאר:

4.3.4.1. אמצעי אבטחת מידע והגנת פרטיות.

4.3.4.2. גיבוי.

4.3.4.3. המשכיות עסקית.

4.3.4.4. אמנת שירות.

4.3.4.5. סיום התקשרות.

4.3.4.6. אחריות הספק לשמירת זמינות המידע, אמינותו, חסיונו, שלמותו של ר"י.

4.3.4.7. סקרים תקופתיים ובקרות

4.3.4.8. זכויות חוזיות.

4.3.4.9. איסוף ראיות דיגיטליות וזימון עובדי הספק לעדות, אם הדבר יידרש

4.3.4.10. ממשקים בין הספק לבין מערכות ר״י.

4.4. פרטיות

4.4.1. הספק יתחייב לשמור/להגן על פרטיות מידע, נכסים (השייכים לר״י) ומערכות אשר ישויכו לרכבת ישראל.

4.4.2. הספק יתחייב לעמוד בהתאם לחוק הגנת פרטיות ותקנות העזר, ובכלל זה נהלי רמו״ט.

4.4.3. כל שינוי במדיניות הספק בנוגע להגנת הפרטיות יובא לאישור ר״י.

4.5. חוקיות התכנה ופלטפורמת מחשוב

4.5.1. הספק יצהיר שכל התוכנות ומערכות המחשוב אשר משמשים אותו לבמתן השירותים לר״י הינם חוקיים, ונמצאים בבעלותו הבלעדית.

4.6. זכויות חוזיות

4.6.1. בהתאם לזכויות החוזיות, רשאית רכבת ישראל:

4.6.1.1. לדרוש דוח על ליקוי אבטחה ו/או ליקויים בתחום הגנת הפרטיות, במידה וקיים חשד ברכבת ישראל על קיומם.

4.6.1.2. להורות לחברה להפסיק העסקתו של עובד זה או אחר, מטעמים הנוגעים לביטחון מערכות המחשוב ומאגרי המידע , המשמשים את רכבת ישראל.

4.6.1.3. לדרוש תיקון ליקויים, אשר יתגלו בסקרי סיכונים, ביקורות מתוכננות, ביקורות פתע , גילוי אקראי או יזום של ליקויי אבטחה , אשר יש להם השלכה על אבטחת מערכות רכבת ישראל והחברה תהיה חייבת לתקן ליקויים אלו תוך פרק זמן סביר (לעניין זה - הזמן המוערך ע״י גופים מקצועיים לתיקון הליקוי). במקרה של ליקויים קריטיים, תידרש החברה לתקן ליקויים אלו באורח מידי.

4.7. הצהרת סודיות

4.7.1. נציג מורשה חתימה מטעם חברת האם, ונציג מורשה מטעם נציג חברת האם במדינת ישראל, יחתמו על הצהרת סודיות עבור הספק ובעצם חתימתם תייצג מחויבותו של הספק לעמוד בכלל ההתחייבויות החוזיות והחוקיות.

4.7.2. כל טפסי הצהרת הסודיות יועברו לרכבת ישראל.

4.8. קניין

4.8.1. כל המידע, התוכנות, האפליקציות, הנתונים, קוד וכו׳ אשר יאוחסנו בענן מחשבי יהיו בבעלותה המלאה והבלעדית של ר״י.

4.8.2. הספק יצהיר כי הוא מוותר על זכותו לתבוע כל זכות קניינית מר״י , ובכלל זה את הזכות לקניין רוחני.

4.9. אמנת שירות

4.9.1. ר״י תקבע אמנת שירות עם הספק אשר תתבסס על זמינות, אמינות וסודיות מידע (נכסי רכבת).

4.9.2. כל שינוי באמנת שירות יובא לאישור ר״י.

4.10. מסירת מידע והסכם חסיון

4.10.1. הספק לא ימסור מידע ממאגרי המידע, ומידע על אבטחת המערכות נשוא ההתקשרות זו לשום גוף או אדם, ללא אישור בכתב מאגף בטחון או מי מטעמו (ממונה אבטחת מידע).

4.10.2. אף אם הספק יקבל צו שיפוטי המתיר לגורם ממשל ו/או גורם צד שלישי לגשת למידע, חובה יהיה על הספק לאפשר לר״י להגיש התנגדות לצו, וזאת לפני מסירת המידע לגורם הממשל ו/או גורם צד שלישי.

4.10.3. הספק יערוך ויקיים נוהל רישום מסודר של העברה/קבלה מידע כלשהוא בנוגע לנכסי ר״י לגורם מוסר/מקבל מידע, תוך רישום פרטי המקבל/מוסר, סוגי רשומות ומועדי מסירה וקבלה, רישום הנ״ל יועבר מדי חצי שנה לעיון לאגף בטחון.

5. מכרז לאספקת מערכת

5.1. על המערכת המסופקת לקיים עקרונות אבטחת מידע כלליים כמו:

5.1.1. קיום מנגנונים מפותחים של זיהוי, אימות והרשאות.

5.1.2. מערכת ההרשאות תפעל על פי העיקרון: "הכול אסור אלא אם כן הוגדר אחרת" (Default Deny Stance).

5.1.3. המערכת תקל ככל האפשר על תחזוקתה, ניהול ההרשאות, המשתמשים שלה וכו' .

5.1.4. המערכת תהיה גמישה ככל הניתן, תאפשר שינוי ברירות מחדל, ופרמטרים.

5.1.5. המערכת תהיה נוחה להתממשקות למערכות חיצוניות לצורך יצוא ויבוא נתונים.

5.1.6. המערכת תספק שירותי ניטור, דיווח ופיקוח נאותים.

5.2. יכולות זיהוי ואימות (identification and authentication)

5.2.1. על הספר לפרט

5.2.1.1. יכולות זיהוי משתמשים במערכת, וכן לבצע אימות שאכן מדובר במשתמש שהזדהה. תהליך זה מתרחש בשלב הראשוני של הכניסה למערכת, לפני שהמשתמש קיבל הרשאות כלשהן למשאבי המערכת. על המשתמש לספק מידע אשר יוכיח את זהותו.

5.2.1.2. המנגנון לזיהוי ואימות משתמשים(גם במהלך session).

5.2.2. **מדיניות סיסמאות**.

5.2.2.1. פירוט כלי המערכת לקביעה ואכיפה של מדיניות סיסמאות מרכזית, לגבי (לפחות) איכות הסיסמא (אורך, תווים חוזרים, תווים עוקבים, QWERTY וכו'), תוקף, ניסיונות גישה כושלים ונעילות ו History-.

5.2.2.2. היכולת לשנות את הסיסמא.

5.2.2.3. המערכת תאפשר לקבוע אילוץ החלפת סיסמא תקופתית.

5.2.2.4. הסיסמא לא תעבור גלויה ברשת.

5.2.3. ייחודיות קבוצות, תיבות, קבוצות משתמשים, מסמכים, תכניות , קבצים וכו' .

5.2.4. יכולת קישוריות לשרתים חיצוניים של זיהוי ואימות לדוגמא:

5.2.4.1. הסתמכות על הזדהות מול מערכת ההפעלה (לדוגמא באמצעות שירותי Active Directory – קרברוס) .

5.2.4.2. התממשקות לשרת Directory מרכזי (LDAP/DAP)

5.2.4.3. התממשקות למנגנוני הזדהות של סיסמא חד פעמית, או כרטיסים חכמים (RADIUS, וכו').

5.2.5. פירוט האם ההסתמכות הינה חד-כיוונית, והאם הרשאות באפליקציה הינן מקור לאסקלציה של הרשאות בפלטפורמות "נמוכות" יותר?

5.2.6. פירוט האם מתבצע באפליקציה ו/או בתוכניות זיהוי hard coded?

5.2.7. פירוט האם כל המשתמשים יהיו ניתנים למחיקה, וכל הסיסמאות ניתנות לשינוי תקופתי.

5.2.8. פירוט על מנגנון הזיהוי והאימות להתממשק למנגנון ה-audit אשר יתואר בהמשך.

5.3. מנגנון הרשאות

5.3.1. הענקת הרשאות הגישה במערכות השונות תתבסס על שיטת ה- DAC (Discretionary Access Control). בשיטה זו יוגדרו הרשאות ספציפיות לאובייקטים במערכת על-פי שמות המשתמשים, שמות קבוצות משתמשים או שניהם יחד. שינוי הרשאות הגישה יתבצע על-ידי גורמים מוסמכים בלבד.

5.3.2. על הספק לפרט את מנגנון ההרשאות של המערכת.

5.3.3. יש לפרט יכולת ניהול הרשאות: ברמת המשתמש, ברמת קבוצת משתמשים, ברמת סוג המידע, ברמת אובייקט (מסך, כפתור, רשומה, שדה), ברמת קבוצות אובייקטים, וכו' .

5.3.4.יש לפרט יכולת קביעת הרשאות מגוונת (read, write, update, delete) ולא רק (access, deny access).

5.3.5.הספק יפרט קיום אפשרות קביעת פרופיל משתמש לכל קבוצה או תפקיד ארגוני ומתן אפשרות לניהול נוח של מערך פרופיל המשתמש. פרופיל המשתמש לא יהיו חשבונות משתמש לגיטימיים במערכת אלא ישמשו להקניית הרשאות בלבד.

5.3.6.יש לפרט אמצעי חלחול ההרשאות שבמערכת (האם שיוך משתמש לקבוצת משתמשים יעביר אליו גם את ההרשאות של הקבוצה, שינוי פרופיל הרשאות ישנה הרשאות לכל מי שמשויך לפרופיל זה, וכו').

5.3.7.יש לפרט גמישות ניהול הרשאות.

5.3.8.יש לפרט יכולות תמיכה במנגנוני הרשאות חיצוניים.

5.4. ניהול משתמשים

5.4.1.חלק קריטי ועיקרי מכל יישום ומערכת הרשאות, הינו מודול ניהול המשתמשים שלו. על הספק להציע מנגנון ניהול הקמת ותחזוקת משתמשים גמיש, ידידותי ונוח.

5.4.2.הספק יפרט את:

5.4.2.1. מנגנוני ניהול המשתמשים של המערכת.

5.4.2.2. תמיכת מערכת ביצירת מבנה הירארכי חכם במערכת ההרשאות, והיכולת לחברו לתוכן הרלוונטי בתוך האפליקציה (מאפשר תחזוקה אוטומטית של משתמשים, עפ"י מקומם ההירארכי).

5.4.2.3. אפשור ניהול חכם של קבוצות (קבוצה בתוך קבוצה, קבוצות חופפות וכו').

5.4.2.4. אפשור יצירת משתמש ע"י העתקת משתמש קיים, או ע"י העתקת פרופיל משתמש.

5.4.2.5. אפשור מחיקת משתמשים מהמערכת.

5.4.2.6. מערכת דוחות גמישה, כמפורט בסעיף הבא.

5.4.2.7. אפשור קליטת משתמשים חדשים וביטול משתמשים בצורה גורפת (Batch).

5.4.2.8. יכולות התממשקות למערכות חיצוניות של ניהול משתמשים. יש לפרט ממשקים מוצעים מול מערכות חיצוניות אשר יאפשרו הפעלת פונקציות (הקמת משתמש, מחיקה, שינוי הרשאות) למשל, בעזרת API או בעזרת פקודות prompt.

5.5. **תיעוד, בקרה והתראה** (log, audit and alert)

5.5.1.מערכת תשלב פתרון לתעד פעילות אשר תוגדר קריטית במערכת, פעילות אשר נראית חריגה (כולל פעילות בבסיס הנתונים ו/או במערכת ההפעלה), ופעילות או ניסיונות לביצוע פעולות אשר נוגדת ישירות policies כפי שהוגדרו במערכת. כמו כן, על המערכת לספק כלים מתאימים לשמירה על קבצים אלו ויכולות דיווח לבעלי התפקידים המתאימים כדי שיוכלו לטפל בהתרעות.

5.5.2.מנגנון הבקרה (Audit) במערכות יאפשר ביצוע מעקב אחר האירועים הבאים:

5.5.2.1. שימוש במנגנון ההזדהות (login/logout, ניסיונות כושלים, וכו').

5.5.2.2. ניסיון כושל בכניסה למערכת.

5.5.2.3. ניסיונות גישה למידע שאין לו הרשאת גישה.

5.5.2.4. אירועים אפליקטיביים שיוגדרו כדורשי בקרה עפ"י מנגנון כללים מיוחד לנושא.

5.5.2.5. התחלת פעילות מסוימת אשר תוגדר כדורשת בקרה על-ידי המשתמש (פתיחת כספת, שליחת מסר וכו').

5.5.2.6. מחיקת אובייקטים במערכת.

5.5.2.7. פעילויות המבוצעות על-ידי גורמים בעלי הרשאות גבוהות.

5.5.2.8. פעולות אדמיניסטרציה (ניהול משתמשים, הורדה והעלאת מערכת, services, וכו').

5.5.2.9. שגיאות תפעוליות (נפילת מערכת, הודעות שגיאות תוכנה, וכו').

5.5.2.10. עבור כל אירוע המוגדר כדורש בקרה יישמרו הפרטים הבאים:

5.5.2.10.1. תאריך ושעה.

5.5.2.10.2. מקור ביצוע הפעולה (דוגמא: כתובת IP, domain)

5.5.2.10.3. שם המשתמש.

5.5.2.10.4. סוג האירוע.

5.5.2.10.5. הצלחה או כישלון של האירוע.

5.5.2.10.6. זיהוי האובייקט עליו מבוצעת הפעולה (דוגמא: שם קובץ).

5.5.2.10.7. תיאור הפעולה (מה בוצע): עבור כל סוג אירוע יש לספק תוכן רלוונטי. למשל: עדכון רשומה, ניסיון גישה לרשומה, מחיקת משתמש, הורדת מערכת, וכו' .

5.5.3. על ההודעות צריכות להיות אמינות, מלאות וברורות.

5.5.4. על הספק לפרט יכולות המערכת לייצא את הנתונים לקונסולה מרכזית (מערכת שו"ב).

5.5.5. על מנגנון הבקרה להתממשק למנגנון הדוחות ולספק רמה גבוהה של דוחות, חיתוך מידע, וכו' .

5.5.6. על הספק לפרט יכולות דיווח של המערכת (במייל, SMS, snmp traps וכו') למנהלי המערכת על אירועים שיוגדרו כדורשי דיווח.

5.5.7. על מערך הבקרה להיות מאובטח כיאות. רק משתמשים מורשים יקבלו גישה אליו, ובמיוחד יש להקפיד על בקרת גישה ליכולת להעלות ולהוריד את מנגנון הבקרה.

5.6. מערכת דוחות

5.6.1. על הספק לפרט בנוגע למערכת דוחות גמישה על המנגנונים הבאים:

5.6.2. דוחות על מערכת ההרשאות (הרשאות למשתמש, משתמשים בקבוצת משתמשים, וכו').

5.6.3. דוחות ממערכת ה-auditing (מספר אירועים מכל סוג, ניסיונות גישה כושלים, וכו').

5.6.4. יכולת יצוא של הקבצים לתוכנות חיצוניות (פורמט XML, DOC, TXT, וכו').

5.6.5. קיום banner המסווג את הדוח, מציין את שם המשתמש שהפיק אותו, תאריך ושעה.

5.6.6. על מערכת הדוחות לאפשור למנהל המערכת להגדיר דוחות חדשים.

5.6.7. על הדוחות להיות קריאים, ברורים ואמינים.

5.7. מניעת התכחשות (Non Repudiation)

5.7.1. על הספק לפרט תמיכה במנגנוני מניעת התכחשות באמצעות חתימה דיגיטאלית על המסרים (בהתאם לחוק החתימה האלקטרונית הישראלי).

5.8. ניתוח פרוטוקולים

5.8.1. על הספק לפרט את הפרוטוקולים המשמשים את האפליקציה בממשק עם תוכנת הלקוח, בזמן ביצוע הזדהות, בממשקים עם בסיס הנתונים, ועם שרתים ומודולים חיצוניים אחרים. על הספק לפרט את אמצעי אבטחת המידע שבפרוטוקולים אלו.

5.9. שלמות הנתונים

5.9.1. במקרים רבים יש לדאוג לכך שיחסים בין נתונים שונים במערכת יישמרו, שמידע לא ייפגם כתוצאה מתהליכי עיבוד ועדכון ממושכים, ושתהליכים יוכלו להיות "משוחזרים". כמו כן, מנגנונים מתאימים צריכים להבטיח שלמות נתונים בעת העברת נתונים בין מערכות, בין משתמשים, או בין אובייקטים במערכת.

5.9.2. על הספק לפרט מנגנונים הקיימים לשלמות נתונים .

5.9.3. על הספק לפרט קיום מנגנוני בדיקה לתהליכי עדכון מסיביים במערכת, השוואה עם גיבוי שלפני הפעולה, הצלבת תוצאות, וכו'.

5.9.4. על הספק לפרט קיום תהליך ניהול תהליכים אשר יאפשר יכולת שיחזור וטיפול של רשומות שסנכרונן נכשל.

5.9.5. על הספק לפרט הפעלת פרוטוקולים של שלמות על נתונים המועברים בין יישומים, ייצוא ויבוא של נתונים. קיום מנגנון מעקב וטיפול בתקלות בחילופי מידע בין מערכות (ראה גם סעיף העברת נתונים בהמשך).

5.9.6. על הספק לפרט קיום מנגנוני אחזור נתונים במקרה של תקלה, שגיאה או מעבר למערכת גיבוי.

5.9.7. על הספק לפרט קיום מנגנוני שלמות נתונים בבסיס הנתונים (למשל, קביעת יחסים בין שדות, referential integrity).

5.10. זמינות

5.10.1. על הספק לפרט אילו מנגנונים יושמו בכדי לשמר זמינות הנתונים.

5.11. סודיות ופרטיות

5.11.1. על הספק לפרט תמיכה בסיווג המידע ובשמירה על חסיון הפרט. פירוט ל:

5.11.2. תמיכה בסוגי מידע שונים(מידע רגיש וכ').

5.11.3. יכולת ציון במערך ההרשאות של מסכים/קבצים/שדות או כל אובייקט אחר כרגיש. על כן, יהיו מסכים אשר לא יוצג בהם מידע רגיש, או מידע אישי למשתמשים מסוימים. לחילופין, יש להגדיר במידת הצורך מסכים נפרדים: אחד הכולל את המידע הרגיש ואחד שלא.

5.11.4. יכולת הגדרה במערכי ה-audit לרישום גישה או ניסיונות גישה למידע המוגדר כרגיש.

5.11.5. יכולת סימון רגישות המידע על דוחות המערכת.

5.11.6. מניעת אפשרות לבקשות לאחזור מידע כלליות, אלא רק בעלת קריטריונים ספציפיים.

5.11.7. יכולת לעצב תהליכים אשר דורשים אישור של יותר מבן-אדם אחד (עקרון חשב-מבקר).

5.11.8. יכולת לערבל (scramble) נתונים המועברים מסביבת ה-production לסביבות אחרות (ראה גם סעיף הפרדה בין סביבות).

5.12. הצפנה

5.12.1. על הספק לפרט לגבי שיטות ההצפנה שבשימוש המערכת:

5.12.1.1. תהליך ורכיבי ההצפנה (מסמכים, מסרים, כספות, בסיס נתונים, ממשקים וכו').

5.12.1.2. פרוטוקולים (כגון: DES, AES, SSL3).

5.12.1.3. תהליכי ניהול מפתחות במערכת.

5.12.1.4. הצפנת קובצי הסיסמאות.

5.12.1.5. הצפנה של המידע העובר ברשת (מול המשתמש ומול מערכות אחרות)

5.12.1.6. הצפנת נתונים המועברים בין יישומים.

5.13. **העברת מידע** (data transmission)

5.13.1. העברת מידע בין ר"י לשאר עולם, ממשקים עם מערכות אחרות, קשר רציף המעדכן מאגרי מידע במקומות שונים, כל אלו הינם מקור לפרצות אבטחת מידע שונות. על הספק לפרט מנגנונים הקיימים למטרות אלו בשידור מידע או העברתו בין אפליקציות בתחומים הבאים:

5.13.2. זיהוי ואימות (Authentication)

5.13.3. בקרת גישה (Access control)

5.13.4. סודיות (Data confidentiality)

5.13.5. שלמות (Data integrity)

5.13.6. מניעת התכחשות (non-repudiation)

5.14. ניהול session

5.14.1. על המערכת לספק פונקציות ניהול session מפותחות על מנת לשמור על יכולת non-repudiation ועל בטחון ה-session (כ- session ניתן להגדיר את מכלול הפעולות אשר המשתמש מבצע מעת ההזדהות וכניסתו למערכת, ועד ליציאה).

5.14.2. על הספק לפרט את מנגנון ניהול ה- session שבמערכת המוצעת.

5.14.3. יש לפרט אילו כלים מתאימים לספק לזיהוי וקיום ה-session בצורה מאובטחת, במטרה למנוע התקפות מסוג session hijacking, ו- man in the middle attacks.

5.14.4. יש לפרט אמצעים להצפנה של הקשר אם קיימים, כדי למנוע האזנה ל-session בין הלקוח לשרת.

5.14.5. יש לספק אמצעים ל-end-to-end identification דרך כל ה-session, גם אם "עובר" דרך שרתים ומודולים שונים, לצורכי היכולת לתיעוד תהליך, ושמירה על עקרון ה- non-repudiation, וכן גם כדי למנוע התקפות כדוגמת אלו בסעיפים קודמים.

5.14.6. הגנה מפני ניסיונות פגיעה

5.14.6.1. הספק יפרט את אמצעי האבטחה אשר יושמו בכדי להגן על נכסי רכבת ישראל.

5.14.6.2. על הספק לפרט תכנית למזעור יכולת פגיעה על ידי עובדי החברה (או נציגה בארץ).

5.14.7. תגובה לאירועי אבטחת מידע

5.14.7.1. הגדרת אירוע אבטחת מידע.

5.14.7.2. אירוע אבטחת מידע שיש לו פגיעה בעלת אופי שיש בו פגיעה בזמינות/אמינות/שרידות/הרשאות נכסי רכבת ומערכותיה יוגדר כאירוע אבטחת מידע חמור.

5.14.7.3. אירוע שקיימת זליגת מידע מנכסי ר"י יוגדר כאירוע אבטחת מידע חמור.

5.14.8. דיווח על אירועי אבטחה

5.14.8.1. במידע ומדובר באירוע בעל אופי שיש בו פגיעה זמינות/אמינות/שרידות/הרשאות/חסיון וזליגת מידע מנכסי רכבת ומערכותיה ידווח ספק במידית לממונה אבטחת מידע.

5.14.9. תגובה וטיפול לאירועי אבטחת מידע

5.14.9.1. הספק יפרט אופן טיפולו בתגובה לאירוע .

5.14.9.2. למען הסר ספק אגף הביטחון בר"י יוגדר כפוסק בכל הנושאים הכוללים את קביעת Severity של אירוע.

5.14.10. תיעוד האירוע

5.14.10.1. הספק יפרט את נושא תיעוד האירוע.

5.14.10.2. תיעוד זה יתבצע יכלול:

5.14.10.2.1. שמירת קבצים רלוונטיים, צילומי מסך ועוד.

5.14.10.2.2. ניהול יומן אירועים לתיעוד האירוע.

5.14.10.2.3. כתיבת דוח בסיום אירוע המתעד את אירוע אבטחת המידע ואת הראיות שנאספו במהלכו ומתעד את הפעילות שבוצעה בנידון. העתק הדוח והראיות יומצאו תוך 48 שעות מזמן סיום האירוע לר״י.

5.15. תיעוד

5.15.1. יישמר תיעוד לגבי תפיסת האבטחה הכוללת של המערכת, מנגנוני האבטחה השונים המיושמים בכל מערכת ותוצאות הבדיקות שנעשו לבחינת יעילות מנגנוני האבטחה. על בסיס עקרונות אלה יבצע הספק אפיון מפורט של מערך אבטחת המידע במערכת המוצעת וכן אפיון כל מערך ההרשאות ע״פ קבוצות משתמש.

5.16. ראיות ועדי הספק

5.16.1. הספק יתחייב להמציא לר״י כל ראיה (דיגיטלית, כתובה או אחרת) תוך 48 שעות מזמן הבקשה.

5.16.2. הספק יתחייב והוא ועובדיו ישתפו פעולה עם גורמי חוק וביטחון במדינת ישראל, ובכלל זה יתייצבו למתן עדות במועדים אשר ר״י ו/או גורמי החוק והביטחון במדינת ישראל יקבעו.

5.16.3. על הספק להבטיח כי הניטור המתבצע ע״י עונה על דרישות חוק דיני הראיות במלואן.

5.17. אבטחת מידע בניהול משאבי אנוש של הספק

5.17.1. אבטחת מידע בתהליכי גיוס עובדים

5.17.1.1. עובדים המגויסים לארגון יעברו בדיקות רקע, אשר מטרתן לאמת את הנתונים שנמסרו על-ידי המועמד/ת.

5.17.1.2. במשרות רגישות הנוגעות במידע, כפי שיוגדרו על-ידי מנהל אבטחת המידע, יבוצעו בדיקות רקע ואמינות נוספות.

5.17.1.3. חוזה הנחתם עם עובדים חדשים יכלול התייחסות לאחריות העובד בכל הנוגע להיבטי אבטחת מידע, וילווה בהצהרת סודיות.

5.17.1.4. חוזה של הארגון עם חברות כוח אדם/השמה או עם חברות המספקות שירותי מיקור חוץ (Outsourcing), יכלול התייחסות בכל הנוגע לבדיקות המבוצעות בתהליכי גיוס העובדים.

5.17.2. אבטחת מידע בעת העסקת עובדים והגברת המודעות שלהם

5.17.2.1. נוהלי אבטחת מידע של הספק יגדירו מהן הפעולות שיש לבצע כדי לשמור על נכסי המידע של הארגון, פעולות אלו יכללו גם אמצעים שינקטו לגבי התקשרות של העובדים מחוץ למקום העבודה.

5.17.2.2. יוגדרו נהלים, בקרות ופעולות נוספות המיועדות למנוע את זליגת המידע מעובדים להם יש נגישות למידע של ר״י.

5.17.2.3. הספק יגדיר תכנית הדרכה להעלאת רמת מודעות העובדים לאבטחת המידע בארגון.

5.17.3. אבטחת מידע בסיום העסקת עובדים

5.17.3.1. לעובדים (כולל עובדים חיצוניים לארגון) המסיימים את העסקתם בארגון, בין אם ביוזמתם או ביוזמת המעסיק, ייחסמו הרשאות הגישה למידע (בין אם למערכות מידע ובין אם לאמצעים פיזיים).

5.17.3.2. ההספק יוודא כי בסיום ההעסקה לא יישארו נכסי מידע של הארגון בידי העובד.

5.17.3.3. הספק יגדיר את אופן הטיפול בעובדים בהיבטי אבטחת מידע לתקופת הזמן שבין הודעת העזיבה לסיום העסקה. יש להגדיר דרישות לפחות בנושאי בקרת גישה, עבודה על מערכות ומסמכים וכו'.