LALUM

חוברת אבטחה

מה פועל, מה נבדק ומה אינו מובטח, עם סקריפט ביקורת ותבניות הקשחה

נבדק ב-10.11.2026

lalumapp.com/security/

ד"ר עו"ד אברהם ללום

כאן מתוארים הבקרות שפועלות בפועל באתר, בפורטל הלקוחות ובמערכת העבודה של הפירמה, ומה כל אחת מהן אינה עושה. כל משפט נבדק מול הקוד, מול המערכת החיה או מול נוסח הדין, ולא נכתב משפט שלא הצלחנו לבדוק.

איך לקרוא את העמוד

- כל טענה נבדקה ב-10.11.2026, אלא אם כתוב בראש הקבוצה שלה תאריך אחר. מערכת משתנה, ולכן התאריך חלק מהטענה.
- טענה שמתארת ספק (למשל מארח מסד הנתונים) היא הצהרת הספק, מסומנת ככזו, ואינה תכונה שבנינו.
- לכל טענה יש רשומת אימות פנימית: מה נבדק, איך, ואיך חוזרים על הבדיקה. אנשי אבטחה ובודקי נאותות מוזמנים לבקש אותה.
- היכן שיש גבול להגנה, הוא כתוב מתחת לטענה עצמה.
- טענה שמצטטת חוק, תקנה או כלל מסומנת "לשון הדין". הציטוט הושווה מילה במילה בשני מקורות בלתי תלויים, ומתחתיו המקור והקישור לנוסח המלא. טענה שמצטטת את מדיניות הפרטיות שלנו מסומנת "מתוך המדיניות".

פיתוח מאובטח

נבדק ב-2.11.2026

SEC-22

שער בדיקה לכל שינוי בקוד

כל בקשת שינוי בקוד (pull request) עוברת שער בדיקה אוטומטי: Gitleaks מחפש סודות בקוד ובהיסטוריה שלו, Semgrep מנתח את הקוד, כללי האבטחה של המאגר בודקים בקרת גישה, הזרקות, סודות והרשאות של סוכני בינה מלאכותית, npm audit ו-pip-audit בודקים תלויות עם חולשות ידועות, Bandit בודק קוד Python ו-ShellCheck בודק סקריפטים. ממצא חדש צובע את הריצה באדום. השער רץ גם על כל מיזוג לענף הראשי ובכל יום שני, והריצה על הענף הראשי ב-2.11.2026 הסתיימה ללא ממצא חדש. הכללים ממופים ל-OWASP Top 10 (2025), ל-OWASP API Security Top 10 (2023), ל-OWASP Top 10 for LLM Applications (2025), לבקרה A.8.28 של ISO/IEC 27001:2022 ול-NIST SP 800-218 (SSDF).

גבול: השער מזהה דפוסים ידועים, ואינו בדיקת חדירה. ממצאים ישנים שנבדקו ונמצאו לא מסוכנים רשומים ברשימת חריגים, כל אחד עם הנימוק שלו. בהגדרות המאגר השער אינו מוגדר עדיין כבדיקת חובה, ולכן הכלל שלא ממזגים שינוי עם ריצה אדומה הוא כלל עבודה. בדיקת התלויות מכסה את האפליקציה ואת שירות ה-webhook הקולי, ולא את כל הפרויקטים המשניים שבמאגר.

SEC-23

ביקורת קוד מלאה

ב-1.11.2026 נבדק כל מאגר הקוד מול אותם תקנים: סריקת סודות בכל היסטוריית השינויים, ניתוח קוד סטטי, קריאה ידנית של כל 45 פונקציות השרת ושל תהליכי האוטומציה, ויועץ האבטחה של מסד הנתונים. התיקונים לממצאים הבאים נפרסו ב-2.11.2026: הרשאת מנהל נקבעת לפי דגל במסד ולא לפי כתובת דוא"ל, פעולות מנהל בפונקציות השרת דורשות אימות דו-שלבי, נתיב קובץ נבדק כך שלא ייצא מהתיקייה של המשתמש, שליחת דוא"ל מוגבלת לכל חשבון בכל שעה, וסוד משותף מושווה בזמן קבוע. ב-5.11.2026 נסגרו עוד ארבעה: דרישת הגורם השני של המנהל הורחבה להרשאות ברמת השורה, מפתח הדוח היומי עבר מכתובת הבקשה לכותרת שלה, וכך גם המפתח שספק החתימה האלקטרונית שולח, והתלויות בפרויקטים המשניים עודכנו. שני התיקונים הראשונים נבדקו באותו יום מול המערכת החיה.

גבול: לא כל הממצאים נסגרו. אחד פתוח: תלות אחת בכלי שרץ רק על מחשב הפירמה ממתינה לגרסה חדשה של הספרייה שמגבילה אותה. בתיקון של ספק החתימה האלקטרונית נבדק מול המערכת החיה שבקשה שמביאה את המפתח בכתובת נדחית. הביקורת נעשתה בידי הפירמה ולא בידי גוף חיצוני.

SEC-24

מנהל הפלטפורמה: דגל במסד וגורם שני

מי שמנהל את הפלטפורמה נקבע רק לפי דגל במסד הנתונים, ולא לפי כתובת דוא"ל שמושווית בקוד. פונקציות השרת שפועלות בהרשאת מנהל דוחות סשן שנכנס בסיסמה בלבד, ודורשות סשן שעבר אימות דו-שלבי. מ-5.11.2026 כך גם ההרשאות ברמת השורה ובאחסון הקבצים שפתוחות למנהל: סשן שנכנס בסיסמה בלבד מקבל בהן את ההרשאות של משתמש רגיל, וחיבור של כלי חיצוני בשם המנהל אינו מקבל הרשאת מנהל כלל.

גבול: הבדיקה החיה ב-5.11.2026 נעשתה מול פונקציית ההרשאה במסד הנתונים, בסשן מדומה של המנהל בגורם אחד ובשני גורמים, ולא בכניסה דרך הממשק.

SEC-26

מאגרי קוד פרטיים

קוד המקור של הפלטפורמה, מבנה מסד הנתונים ופונקציות השרת נמצאים במאגרי קוד פרטיים, ואינם גלויים לציבור.

גבול: מי שמחובר למאגרים רואה את הקוד: בעל הפירמה, וכלי הפיתוח והפריסה שמחוברים אליהם. סריקת הסודות המובנית של GitHub אינה זמינה למאגר פרטי של חשבון אישי, ולכן הבדיקה לסודות היא Gitleaks בשער שבסעיף הראשון, שרץ על כל שינוי, על כל מיזוג לענף הראשי ובכל יום שני.

זהות והרשאות

SEC-01

כניסה מאומתת

אזור הלקוחות, פורטל הלקוח וסביבת העבודה של הפירמה דורשים התחברות. העוזר המשפטי באתר פועל רק למשתמש מחובר: פנייה אנונימית מקבלת בקשת התחברות ולא מגיעה למודל.

גבול: כלי ניתוח החוזים הציבוריים אינם דורשים התחברות. הם מתוארים בקבוצה "בינה מלאכותית".

SEC-02

אימות דו-שלבי שהמסד אוכף

לשותפים ולעורכי דין זמין אימות דו-שלבי באפליקציית אימות (TOTP), ובחשבון הפירמה הוא מוגדר כחובה. את הדרישה אוכף מסד הנתונים עצמו ולא רק הממשק: רשומות רגישות כגון בדיקות זיהוי לקוח, גרסאות מסמכים ונספחים נדחות מסשן שלא עבר את הגורם השני. חריג אחד, בהחלטת הבעלים: חשבון הנהלת החשבונות החיצונית נכנס בסיסמה בלבד. לחשבון הזה אין גישה לתיקים, למסמכים או לרשומות הרגישות שלעיל, והוא מוגבל לצפייה והורדה של חומרי הנהלת החשבונות.

גבול: חשבון שנכנס בסיסמה בלבד חשוף יותר לדליפת סיסמה, ולכן ההרשאה שלו מוגבלת מראש לקריאה בלבד.

SEC-03

קודי שחזור

בהפעלת האימות נוצרים שמונה קודי שחזור חד-פעמיים, ומוצגים פעם אחת. הקוד עצמו אינו נשמר, אלא גיבוב SHA-256 הקשור לחשבון. חמישה ניסיונות שגויים נועלים את השחזור לחמש עשרה דקות. שחזור מסיר את גורמי ה-TOTP הקיימים, כדי שאפשר יהיה לחבר אפליקציה חדשה.

SEC-04

הרשאת מנהל נקבעת רק בשרת

דגל מנהל הפלטפורמה אינו ניתן לשינוי מסשן של משתמש, גם לא של המשתמש עצמו, ואינו ניתן להגדרה בעת הרשמה. הוא נקבע רק בצד השרת.

SEC-20

סיסמאות: בחירה, החלפה ואיפוס

סיסמה חדשה, בהרשמה, בהחלפה ובאיפוס, חייבת לכלול לפחות 12 תווים ולא יותר מ-72 בתים. אין חובה לסימנים מיוחדים. הטופס חוסם סיסמאות נפוצות, חזרות ורצפי מקלדת, וסיסמה שבנויה מכתובת האימייל או מהשם של החשבון. הוא בודק גם אם הסיסמה הופיעה בדליפה פומבית, בשיטה שבה יוצאים מהדפדפן רק חמשת התווים הראשונים של גיבוב הסיסמה. בטופס ההחלפה צריך להזין את הסיסמה הנוכחית, והיא נבדקת מול שרת האימות. אחרי החלפה או איפוס, כל שאר ההתחברויות של החשבון מנותקות. אפשר לאפס סיסמה גם בקוד חד-פעמי שנשלח במייל, ובחשבון עם אימות דו-שלבי נדרש גם קוד האפליקציה לפני שאפשר לבחור סיסמה חדשה.

גבול: הבדיקות שבטופס, כולל בדיקת הדליפה וההשהיה אחרי ניסיונות שגויים, רצות בדפדפן. פנייה ישירה לממשק ההרשמה של ספק האימות עוקפת אותן: שם נאכפים רק מינימום של 12 תווים ובדיקת הסיסמאות המדולפות של הספק עצמו, ולא החסימה של סיסמאות נפוצות, חזרות ורצפי מקלדת. גם הדרישה להזין את הסיסמה הנוכחית נאכפת בטופס ולא בשרת.

SEC-21

בדיקת אבטחה אוטומטית, פעם בשבוע

בכל יום שני בבוקר רצה בדיקה אוטומטית שאינה נוגעת בנתונים. היא מריצה את בדיקות מדיניות הסיסמאות, בונה את האתר וסורקת את הקוד שנשלח לדפדפן לחיפוש מפתח שירות, מפתח ספק או מפתח פרטי. אחר כך היא פונה לאתר החי ובודקת שהוא שולח כותרות אבטחה, שקריאה אנונימית לעוזר האתר מקבלת בקשת התחברות ולא תשובה, ושאישור תשלום בלי הסוד המשותף נדחה. תוצאת כל ריצה נשלחת לפירמה, וכשל בבדיקה מסמן את הריצה באדום. הריצות הידניות שהופעלו ב-20.10.2026 וב-21.10.2026 הסתיימו ללא כשל.

גבול: הבדיקה סוקרת ארבעה דברים בלבד. היא אינה בודקת את מסד הנתונים (הרשאות שורה, מדיניות וגישה), שנבדקים בנפרד בבדיקת SQL ידנית, ואינה מחליפה בדיקת חדירה.

בידוד בין לקוחות ובין משרדים

SEC-05

אבטחה ברמת שורה בכל הטבלאות

בכל טבלאות הנתונים מופעלת אבטחה ברמת שורה (Row Level Security): 147 מתוך 147 בבדיקה מיום 10.11.2026. הגישה לתיק מותנית בתפקיד ובשיוך לפירמה, והיא נאכפת במסד הנתונים ולא רק בממשק.

גבול: הפעלת המנגנון בכל טבלה אינה הוכחה שכל מדיניות נכונה. לכן נכתבו בדיקות SQL ייעודיות לבידוד בין תיקים, חיוב וגישה לפי תפקיד, והן חלק מהקוד.

SEC-06

שמות לקוחות מוסתרים כברירת מחדל

במסכי הצוות מוצג קוד תיק במקום שם הלקוח. חשיפת השם היא פעולה מכוונת שמותרת למנהל הפירמה בלבד, וגם לשותף או לעורך דין שמנהל הפירמה אישר לכך במפורש, אחרי אימות דו-שלבי עדכני. היא דורשת בחירת סיבה, ונרשמת ביומן הביקורת עם מי חשף ולמה, וגם סיום החשיפה ואישור ההרשאה נרשמים.

גבול: זו בקרה ברמת התצוגה. הרשאת הקריאה לתיק עצמו נקבעת במסד הנתונים, כמתואר בסעיף הקודם. הנהלת החשבונות החיצונית רואה את פרטי הלקוח המחויב במסמכים הכספיים ואת תנועות חשבון הבנק העסקי, לקריאה בלבד, כנדרש לניהול ספרים ולהתאמת בנק. אין לה גישה לתיקים.

SEC-07

סודות נשארים בשרת

מפתח השירות הפריבילגי של מסד הנתונים נמצא רק במשתני הסביבה של פונקציות השרת. חבילת הקוד שנשלחת לדפדפן נבדקה, ולא נמצאו בה מפתח שירות, מפתחות של ספקים או מפתחות פרטיים. בדפדפן יושב המפתח הציבורי בלבד, וההגנה על הנתונים נשענת על הסעיף הקודם.

מסמכים וקבצים

SEC-08

מאגרי קבצים פרטיים וקישורים קצרי מועד

כל שמונת מאגרי הקבצים במערכת מוגדרים פרטיים. פתיחת קובץ מהפורטל, ופתיחת מקור של מסמך על ידי שותף או עורך דין, נעשות בקישור חתום שתוקפו שישים שניות.

גבול: קישורי עבודה פנימיים של צוות הפירמה יכולים להיות בני תוקף ארוך יותר, עד שעה. חריג אחד: כשלקוח מעלה קובץ לפורטל, הפירמה מקבלת הודעת דוא"ל עם קישור הורדה שתקף 72 שעות, וכל מי שמחזיק בהודעה יכול להוריד בו את הקובץ עד שיפוג. חותם חיצוני רואה את המסמך שנשלח אליו לחתימה בקישור שתקף עשר דקות.

SEC-09 · הצהרת ספק

הצפנה במנוחה ובמעבר

ספק מסד הנתונים והאחסון, Supabase, מצהיר שהנתונים מוצפנים במנוחה ובמעבר.

גבול: זו הצהרת הספק ולא תכונה שבנינו. היא מכסה את הנתונים שבתוך הפלטפורמה שלו.

https://supabase.com/docs/guides/deployment/shared-responsibility-model

SEC-10 · הצהרת ספק

הסמכת הספק

Supabase מצהירה שהיא עומדת בתקן SOC 2 Type 2 ונבדקת אחת לשנה על ידי גורם חיצוני.

גבול: ההסמכה היא של הספק בלבד. לפי הספק עצמו היא אינה עוברת לסביבות שמחוץ לפלטפורמה, ואינה הסמכה של LALUM.

https://supabase.com/docs/guides/security/soc-2-compliance

תשלומים וחיבורים לצד שלישי

SEC-11

פרטי כרטיס אשראי לא עוברים אצלנו

באפליקציה אין שדות להזנת פרטי כרטיס אשראי. הזנת הפרטים מתבצעת אצל חברת הסליקה, ופרטי כרטיס אינם נשמרים במסד הנתונים של LALUM.

SEC-12

אימות אישורי תשלום

אישור תשלום מחברת הסליקה נקלט רק עם סוד משותף, שנבדק בהשוואה בזמן קבוע, ונדחה כשהסוד אינו מוגדר. כשהאישור כולל סכום, הוא חייב להתאים לסכום אבן הדרך, ואחרת האבן דרך לא מסומנת כמשולמת.

גבול: האימות הוא סוד משותף ולא חתימה קריפטוגרפית של הספק על כל הודעה.

SEC-13

אימות הודעות נכנסות מספקים אחרים

הודעות WhatsApp נקלטות רק עם חתימת HMAC-SHA256 תקפה של Meta, ונדחות כשהסוד אינו מוגדר. ה-webhook הקולי וה-webhook של החתימה האלקטרונית נדחים כשהסוד שלהם אינו תואם או אינו מוגדר.

דפדפן ורשת

SEC-14

כותרות אבטחה ומדיניות תוכן אוכפת

האתר מוגש ב-HTTPS עם HSTS לשנה הכולל תתי דומיינים. מדיניות תוכן (CSP) אוכפת, ולא רק מדווחת, אוסרת סקריפטים מקוונים ואובייקטים, מגבילה מאיפה נטענים סקריפטים, ומונעת הטמעת האתר במסגרת של אתר זר. מוגדרות גם כותרות nosniff, מדיניות רפרר, מדיניות הרשאות דפדפן ובידוד חלונות.

גבול: המדיניות מתירה סגנונות מקוונים. סקריפטים נטענים רק מהמארחים הרשומים בה, ובהם שירותי צד שלישי של האתר הציבורי.

מניעת ניצול לרעה

SEC-15

מגבלות קצב

טפסי הפנייה, קביעת פגישה, ניתוח החוזים והעוזר המשפטי מוגבלים לפי מקור הפנייה. לעוזר המשפטי יש גם מכסה יומית לכל משתמש ומכסה יומית כוללת. כתובת ה-IP של מבקר אינה נשמרת: נשמר גיבוב שמשמש את המגבלה בלבד.

תיעוד, יושרה ושמירה

SEC-16

יומן ביקורת בשרשרת גיבובים

כל רשומה ביומן הביקורת של פירמה כוללת גיבוב SHA-256 של הרשומה שלפניה, ויש פונקציית בדיקה שמאתרת את הרשומה הראשונה שבה השרשרת נשברת. עדכון או מחיקה של רשומה נדחים בידי המסד, וכתובת דוא"ל אינה נרשמת ביומן.

גבול: השרשרת מגלה שינוי בדיעבד, והיא אינה אחסון חיצוני בלתי ניתן לשינוי.

SEC-17

מחיקה לפי תקופות שמירה

משימות מתוזמנות רצות בכל יום: מחיקת מסמכי תיק שהלקוח הסכים למחיקתם שלושים יום אחרי סיום הטיפול, אלא אם חל עיכוב משפטי, והמחיקה נרשמת ביומן הביקורת. מחיקת פניות מהאתר בתום תקופת השמירה שלהן. ריקון תוכן הודעות WhatsApp אחרי שלושים יום, כשמועד וכיוון ההודעה נשארים. ופינוי רשומות זמניות של מנגנון הסרת הזיהוי.

בינה מלאכותית

SEC-18

הסרת פרטים מזהים לפני ניתוח

במערכת העבודה של הפירמה שמות לקוחות וכתובות מוחלפים באסימונים כגון [CLIENT_NAME_2] לפני שהטקסט נשלח לניתוח, והמיפוג חזרה לשמות האמיתיים נשמר בדפדפן למשך הסשן בלבד ומופעל בייצוא.

גבול: הזיהוי מבוסס כללים וזיהוי תבניות, ואינו מבטיח זיהוי של כל פרט. לכן ההחלטה המקצועית נשארת בידי עורך דין, והסרת הזיהוי היא שכבת הגנה ולא תחליף לשיקול דעת.

SEC-19

כלים ציבוריים: שימו לב למה שמעלים

כלי ניתוח החוזים הציבוריים באתר פועלים ללא התחברות ושולחים את הטקסט שהוזן אליהם לספק בינה מלאכותית חיצוני לצורך הניתוח. אין להזין אליהם מסמכים חסויים או מידע מזהה של אחרים.

גבול: פלטי הכלים אינם ייעוץ משפטי ואינם מחליפים עורך דין.

פרטיות, סודיות וחיסיון

נבדק ב-5.11.2026

SEC-27 · לשון הדין

חיסיון עורך דין ולקוח

סעיף 90 לחוק לשכת עורכי הדין קובע: "דברים ומסמכים שהוחלפו בין לקוח לבין עורך דין ויש להם קשר עניני לשירות המקצועי שניתן על ידי עורך הדין ללקוח, לא יגלה אותם עורך הדין בכל הליך משפטי, חקירה או חיפוש, מלבד אם ויתר הלקוח על חסינותם." לפי לשון הסעיף, הוויתור בידי הלקוח.

גבול: החיסיון הוא הוראת דין ולא בקרה טכנית, והמערכת אינה מכריעה מה חסוי. הבקרות שמגינות על חומרי התיק מתוארות בסעיפים SEC-05, SEC-06 ו-SEC-18.

מקור: סעיף 90 לחוק לשכת עורכי הדין, התשכ"א-1961

SEC-28 · לשון הדין

חובת הסודיות של עורך הדין ושל העובדים בשירותו

כלל 19 קובע: "עורך דין ישמור בסוד כל דבר שיובא לידיעתו בידי לקוח או מטעמו, תוך כדי מילוי תפקידיו, זולת אם הסכים הלקוח במפורש אחרת; הוראה זו אינה חלה על גילוי בהליך משפטי, חקירה או חיפוש שאינו חסוי על פי סעיף 90 לחוק." כלל 20 מוסיף: "עורך דין יעמיד את העובדים בשירותו על חובתם לשמור על סודיות הענינים המגיעים לידיעתם במהלך עבודתם." במערכת, הגישה לתיק נקבעת לפי תפקיד ושיוך לפירמה (SEC-05), ולחשבון הנהלת החשבונות החיצונית אין גישה לתיקים (SEC-02).

גבול: החובה מוטלת על עורך הדין ועל העובדים בשירותו. בקרות הגישה במערכת תומכות בה, ואינן ממלאות אותה במקומם.

מקור: כללים 19 ו-20 לכללי לשכת עורכי הדין (אתיקה מקצועית), התשמ"ו-1986

עמידה בדין: פרטיות ואבטחת מידע

נבדק ב-5.11.2026

SEC-29 · לשון הדין

הזכות לעיין במידע

סעיף 13(א) לחוק הגנת הפרטיות קובע: "כל אדם זכאי לעיין בעצמו (...) במידע האישי שעליו המוחזק במאגר מידע." לפי אותו סעיף, אפשר לעיין גם באמצעות בא כוח שהורשה בכתב או באמצעות אפוטרופוס. סעיף 13(ג1) מסייג: "אין בהוראות סעיף זה כדי לחייב למסור מידע אישי בניגוד לחסיון שנקבע לפי כל דין, אלא אם כן המבקש הוא מי שהחסיון נועד לטובתו." בקשת עיון במידע שמוחזק אצלנו נשלחת אל avraham@lalum.co, כפי שכתוב במדיניות הפרטיות (SEC-33).

גבול: הסימן (...) מחליף את המילים על בא כוח ועל אפוטרופוס, שמתוארות אחרי הציטוט. העמוד אינו מתאר מועדי מענה או סדרי בקשה, ואינו מפרש את הסייג מעבר ללשונו.

מקור: סעיפים 13(א) ו-13(ג1) לחוק הגנת הפרטיות, התשמ"א-1981

SEC-30 · לשון הדין

תיקון ומחיקה של מידע

סעיף 14(א) לחוק קובע: "אדם שעיין במידע האישי שעליו ומצא כי אינו נכון, שלם, ברור או מעודכן, רשאי לפנות לבעל השליטה במאגר המידע (...) בבקשה לתקן את המידע האישי או למוחקו." גם בקשה כזו נשלחת אל avraham@lalum.co.

גבול: הסימן (...) מחליף את ההוראה על בעל שליטה שהוא תושב חוץ, שהושמטה מהציטוט.

מקור: סעיף 14(א) לחוק הגנת הפרטיות, התשמ"א-1981

SEC-31 · לשון הדין

תקנות אבטחת המידע ומאגר של עורך דין

לפי תקנה 21(4), על "מאגר המנוהל בידי יחיד" חלה רשימה מצומצמת של תקנות. אבל ההגדרה שבתקנה 1 מוציאה ממנו במפורש "מאגר מידע הכולל מידע שבעל המאגר כפוף בשלו לחובת סודיות מקצועית לפי דין או לפי עקרונות של אתיקה מקצועית". מאגר התיקים של הפירמה כולל מידע כזה (SEC-28), ולכן הרשימה המצומצמת אינה חלה עליו. בכל אחת משלוש רמות האבטחה האחרות שבתקנה 21 חלות תקנה 2, שלפיה בעל המאגר יגדיר "מסמך הגדרות מאגר", ותקנה 4(א), שלפיה הוא יקבע "נוהל אבטחת מידע".

גבול: העמוד מצטט את התקנות ואינו קובע איזו משלוש הרמות חלה על מאגר הפירמה. הבקרות שבעמוד לא מופו לתקנות ולא נבדקו מולן בידי גורם חיצוני.

מקור: תקנות 1, 2, 4(א) ו-21 לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017

ההתחייבויות שלנו, כפי שפורסמו

נבדק ב-5.11.2026

הסעיפים כאן מצטטים את מדיניות הפרטיות שמפורסמת באתר. הנוסח הקובע הוא נוסח המדיניות עצמה.

SEC-32 · מתוך המדיניות

המידע אינו נמכר, וענייני לקוח בחיסיון

מדיניות הפרטיות קובעת: "אנחנו לא מוכרים את המידע שלכם. ענייני לקוח מוחזקים תחת חיסיון עורך דין ולקוח."

גבול: החיסיון עצמו נובע מהדין (SEC-27), ולא מהמדיניות.

מקור: מדיניות הפרטיות באתר

SEC-33 · מתוך המדיניות

עיון, תיקון ומחיקה: למי פונים

מדיניות הפרטיות קובעת: "יש לכם זכות לדעת איזה מידע אישי מוחזק אצלנו עליכם, לעיין בו, ולבקש לתקן או למחוק אותו. למימוש הזכויות, פנו אלינו בכתובת avraham@lalum.co."

גבול: הזכויות עצמן קבועות בחוק (SEC-29, SEC-30), והמדיניות מפנה למימושן.

מקור: מדיניות הפרטיות באתר

מה העמוד הזה אינו טוען

- אין כאן טענה שמערכות LALUM עברו תקן או הסמכה כגון ISO 27001 או SOC 2. ההסמכה שמוזכרת למטה היא של הספק, ואינה עוברת אלינו.
- אין כאן טענה לבדיקת חדירה חיצונית שפורסמה.
- אין סריקת נוזקות אוטומטית של קבצים שלקוח מעלה לפורטל. הקבצים נשמרים במאגר פרטי עם מגבלת גודל ונפתחים בקישור חתום בלבד.
- אין כאן הבטחה שמערכת מסוימת חסינה. אף מערכת אינה חסינה, והעמוד מתאר בקרות ולא ערבות.
- אין כאן טענות על הגדרות שבידי ספקים ושלא נבדקו מול המערכת, לרבות תצורת רשת הפצה וחומת אש ברמת הדומיין.
- השורה שבתחתית כל עמוד מציינת את התקנים ששער הבדיקה של הקוד בנוי לפיהם. היא אינה הסמכה לתקנים האלה ואינה תוצאה של ביקורת חיצונית.

- אין כאן טענה שהמערכת או הפירמה נבדקו בידי גורם חיצוני מול חוק הגנת הפרטיות או מול תקנות אבטחת המידע. הסעיפים שמצטטים דין מביאים את לשונו כפי שאומתה, ואינם חוות דעת משפטית.

בדקו בעצמכם: סקריפט ותבניות

שלושה דברים שאפשר לקחת ולהשתמש בהם. לכל אחד כתוב אם הוא רץ אצלנו או שהוא תבנית, ומה תוקן בהשוואה לגרסאות נפוצות.

TPL-01 סקריפט ביקורת למסד Supabase (רץ אצלנו)

שאילתת קריאה בלבד אחת שמריצים ב-SQL Editor של Supabase. היא לא משנה דבר, ומחזירה רשימת מוקדים לבדיקה לפי חומרה. הרצנו אותה על מסד הנתונים של LALUM ב-19.10.2026.

- בודק: טבלאות ללא RLS, מדיניות פתוחה (true) ל-anon ול-PUBLIC, פונקציות SECURITY DEFINER הזמינות לאורחים או ללא search_path קבוע, Views שעוקפים RLS, מאגרי קבצים ציבוריים, ומדיניות פתוחה לכל משתמש מחובר.
- התוצאה אצלנו: אפס טבלאות ללא RLS, אפס פונקציות או Views חשופים לאורחים, אפס מאגרי קבצים ציבוריים. נשארו מוקד אחד בחומרה גבוהה ומוקד אחד בינונית, ושניהם נתוני ייחוס שמיועדים להיות פתוחים: שלושה קריטריוני ניתוח חוזים לדוגמה ורשימת מחירים. וכן חמש פונקציות עזר לבדיקה ידנית, שמחזירות ערך פשוט בלבד (כן או לא, או סטטוס).
- כל שורה היא מוקד ולא פסק דין. מוקדי REVIEW ו-MEDIUM דורשים החלטה אנושית אם הגישה הפתוחה מכוונת.

```
-- ============================================================================
-- LALUM: Supabase security audit (read only)
-- Paste into the Supabase SQL Editor and run. It changes nothing: one SELECT.
--
-- Checks (severity in brackets):
--   1  Tables in public with Row Level Security off                    [CRITICAL]
--   2  Policies open to everyone (USING/CHECK true) for anon or PUBLIC [HIGH]
--   3  SECURITY DEFINER functions callable by anon or PUBLIC           [HIGH]
--   4  Views that bypass RLS (not security_invoker) and are readable   [HIGH]
--   5  Public storage buckets                                          [HIGH]
--   6  Policies open to every signed in user (USING/CHECK true)        [MEDIUM]
--   7  Anonymous write policies with no identity check                 [MEDIUM]
--   8  SECURITY DEFINER functions with no search_path pinned           [MEDIUM]
--   9  SECURITY DEFINER functions for signed in users, no guard found  [REVIEW]
--  10  Tables with RLS on and no policy; policies for PUBLIC that      [INFO]
--      call an auth helper (fail for anon, so only a naming nit)
--  11  Extensions installed in public                                  [LOW]
--
-- Reading the result: every row is a lead, not a verdict. Row 6 and row 9 need a
-- human to decide whether the open access is intended (a public price list is;
-- an internal playbook is not). Row 9 is a heuristic: it looks for a call to an
-- auth or role helper inside the function body. Edit guard_pattern below to the
-- names of your own helpers. A match does not prove the check is correct, and a
-- miss does not prove it is missing.
-- ============================================================================

with
settings as (
  select '(auth\.(uid|jwt|role)\
(|_is_admin|_my_role|_my_firm_id|_mgr_ok|_fin_can|_is_partner_of|_is_staff_on|_can_view_matter|_client_can|
_matter_firm|_admin_ok|_mfa_ok)'::text as guard_pattern
```

```
),
tbl as (
  select c.oid, c.relname, c.relrowsecurity as rls
  from pg_class c
  join pg_namespace n on n.oid = c.relnamespace
  where n.nspname = 'public' and c.relkind in ('r', 'p')
),
pol as (
  select schemaname, tablename, policyname, permissive, cmd,
         roles::text[] as roles,
         lower(btrim(coalesce(qual, ''))) as q,
         lower(btrim(coalesce(with_check, ''))) as wc
  from pg_policies
  where schemaname in ('public', 'storage')
),
findings as (
  select 1 as rank, 'CRITICAL' as severity, 'RLS disabled' as category,
         'public.' || relname as object,
         'Row Level Security is off: anyone holding the anon key can read and write, per the table grants.'
as detail,
         'ALTER TABLE public.' || quote_ident(relname) || ' ENABLE ROW LEVEL SECURITY;' as fix
  from tbl where not rls

  union all
  select 2, 'HIGH', 'Open policy for anon or PUBLIC',
         schemaname || '.' || tablename,
         'policy "' || policyname || '" ' || cmd || ' to {' || array_to_string(roles, ',') || '} using ['
|| q || '] check [' || wc || ']',
         'Replace true with an ownership or tenant condition, or drop the policy.'
  from pol
  where permissive = 'PERMISSIVE' and (q = 'true' or wc = 'true') and roles && array['public', 'anon']

  union all
  select 2, 'HIGH', 'SECURITY DEFINER callable by anon or PUBLIC',
         p.oid::regprocedure::text,
         'Any visitor can call this function and it runs with its owner''s rights.',
         'REVOKE EXECUTE ON FUNCTION ' || p.oid::regprocedure::text || ' FROM PUBLIC, anon;'
  from pg_proc p
  where p.pronamespace = 'public'::regnamespace and p.prosecdef
    and has_function_privilege('anon', p.oid, 'execute')

  union all
  select 2, 'HIGH', 'View bypasses RLS',
         'public.' || c.relname,
         case c.relkind when 'm' then 'Materialized views are not subject to RLS.' else 'View runs with its
owner''s rights (' || pg_get_userbyid(c.relowner) || ') and ignores the caller''s RLS.' end,
         case c.relkind when 'm' then 'REVOKE SELECT ON public.' || quote_ident(c.relname) || ' FROM anon,
authenticated;'
                       else 'ALTER VIEW public.' || quote_ident(c.relname) || ' SET (security_invoker =
true);' end
  from pg_class c
  where c.relnamespace = 'public'::regnamespace and c.relkind in ('v', 'm')
    and not exists (select 1 from unnest(coalesce(c.reloptions, '{}')) o where o ~ '^security_invoker=
(true|on|1)$')
    and (has_table_privilege('anon', c.oid, 'select') or has_table_privilege('authenticated', c.oid,
'select'))

  union all
  select 2, 'HIGH', 'Public storage bucket', 'storage.' || id,
         'Files in this bucket are readable by URL without any signature.',
         'UPDATE storage.buckets SET public = false WHERE id = ' || quote_literal(id) || ';'
  from storage.buckets where public

  union all
  select 3, 'MEDIUM', 'Open policy for every signed in user',
```

```
         schemaname || '.' || tablename,
         'policy "' || policyname || '" ' || cmd || ' to {' || array_to_string(roles, ',') || '} using ['
|| q || '] check [' || wc || ']',
         'If sign-up is open this means any stranger. Restrict to a role or tenant, unless the data is
meant to be public.'
  from pol
  where permissive = 'PERMISSIVE' and (q = 'true' or wc = 'true')
    and roles && array['authenticated'] and not (roles && array['public', 'anon'])

  union all
  select 3, 'MEDIUM', 'Anonymous write policy, no identity check',
         pl.schemaname || '.' || pl.tablename,
         'policy "' || pl.policyname || '" ' || pl.cmd || ' to {' || array_to_string(pl.roles, ',') || '}
using [' || pl.q || '] check [' || pl.wc || ']',
         'A visitor with no account may write here. Confirm it is meant to, and that the check limits
what.'
  from pol pl, settings s
  where pl.permissive = 'PERMISSIVE' and pl.cmd in ('INSERT', 'UPDATE', 'DELETE', 'ALL')
    and pl.roles && array['public', 'anon'] and not (pl.q = 'true' or pl.wc = 'true')
    and (pl.q || ' ' || pl.wc) !~* s.guard_pattern

  union all
  select 5, 'INFO', 'Policy applies to PUBLIC but requires an identity',
         pl.schemaname || '.' || pl.tablename,
         'policy "' || pl.policyname || '" ' || pl.cmd || ' has no TO clause, so it covers PUBLIC, but its
condition calls an auth or role helper and fails for anon.',
         'Optional: add TO authenticated so the intent is explicit.'
  from pol pl, settings s
  where pl.permissive = 'PERMISSIVE' and pl.cmd in ('INSERT', 'UPDATE', 'DELETE', 'ALL')
    and pl.roles && array['public', 'anon'] and not (pl.q = 'true' or pl.wc = 'true')
    and (pl.q || ' ' || pl.wc) ~* s.guard_pattern

  union all
  select 3, 'MEDIUM', 'SECURITY DEFINER without a pinned search_path',
         p.oid::regprocedure::text,
         'A mutable search_path lets a caller shadow objects the function relies on.',
         'ALTER FUNCTION ' || p.oid::regprocedure::text || ' SET search_path = public, pg_temp;'
  from pg_proc p
  where p.pronamespace = 'public'::regnamespace and p.prosecdef
    and not exists (select 1 from unnest(coalesce(p.proconfig, '{}')) cfg where cfg like 'search_path=%')

  union all
  select 4, 'REVIEW', 'SECURITY DEFINER for signed in users, no guard found',
         p.oid::regprocedure::text,
         'Callable by any signed in user and no call to an auth or role helper was found in the body
(heuristic).',
         'Read the function. Add an explicit check on auth.uid() or a role, or revoke EXECUTE from
authenticated.'
  from pg_proc p, settings s
  where p.pronamespace = 'public'::regnamespace and p.prosecdef
    and has_function_privilege('authenticated', p.oid, 'execute')
    and not has_function_privilege('anon', p.oid, 'execute')
    and pg_get_functiondef(p.oid) !~* s.guard_pattern

  union all
  select 5, 'INFO', 'RLS on, no policy', 'public.' || t.relname,
         'Deny all for the API roles. Correct if only server code with the service role reads this table.',
         'None needed if intended.'
  from tbl t
  where t.rls and not exists (select 1 from pg_policies pp where pp.schemaname = 'public' and pp.tablename
= t.relname)

  union all
  select 6, 'LOW', 'Extension in public', e.extname,
         'Extensions in public widen the API surface.',
```

```
        'ALTER EXTENSION ' || quote_ident(e.extname) || ' SET SCHEMA extensions;'
  from pg_extension e join pg_namespace n on n.oid = e.extnamespace
  where n.nspname = 'public'
)
select severity, category, object, detail, fix
from findings
order by rank, category, object;
```

מה תוקן לעומת גרסאות נפוצות

- גרסה נפוצה של בדיקה כזו מתמקדת רק במדיניות שפתוחה ל-anon. היא מפספסת מדיניות true ל-authenticated, ובהרשמה פתוחה זה כל אדם זר.
- גרסה נפוצה ממיינת את החומרות לפי אלפבית, ואז WARNING מופיע לפני CRITICAL. כאן מיון לפי דירוג מספרי.
- מדיניות בלי סעיף TO חלה על PUBLIC, אבל אם התנאי שלה דורש זהות מחוברת היא נכשלת לאורח. כאן היא מסווגת כהערה ולא כפרצה.

TPL-02 מאגר קבצים פרטי עם מדיניות בעלות (תבנית לביצוע)

תבנית למאגר שבו כל משתמש רואה רק את התיקייה שלו, עם מגבלת גודל וסוגים. שמונת מאגרי הקבצים של LALUM פרטיים, ומדיניות הגישה אליהם נבנתה על אותו עיקרון: ב-client-files לפי בעלות, וב-matter-originals לפי פירמה, תפקיד ואימות דו-שלבי.

- הגישה לקובץ נעשית בקישור חתום קצר מועד (createSignedUrl), לא בכתובת ציבורית. אצלנו הקישורים בפורטל תקפים שישים שניות.
- בגישה לפי פירמה ולא לפי משתמש בודד, משווים את התיקייה הראשונה לפונקציית השיוך שלכם, בטקסט: (storage.foldername(name))[1] = (select public.my_firm_id())::text. כך עובד matter-originals אצלנו.
- אצלנו לכל מאגר יש מגבלת גודל. ב-client-files היא 25MB ואין רשימת סוגים, ורשימת סוגים מותרים מוגדרת ב-matter-originals ובשלושת המאגרים של מסמכי הכספים והחתימה האלקטרונית.

```
-- A private bucket with an owner folder. Replace the bucket id and the types.
insert into storage.buckets (id, name, public, file_size_limit, allowed_mime_types)
values ('client-documents', 'client-documents', false, 10485760,
        array['application/pdf', 'image/jpeg', 'image/png'])
on conflict (id) do update
  set public = false,
      file_size_limit = excluded.file_size_limit,
      allowed_mime_types = excluded.allowed_mime_types;

-- The first folder of every object path is the owner's user id.
create policy "documents: read own" on storage.objects
  for select to authenticated
  using (bucket_id = 'client-documents'
         and (storage.foldername(name))[1] = (select auth.uid())::text);

create policy "documents: upload to own folder" on storage.objects
  for insert to authenticated
  with check (bucket_id = 'client-documents'
              and (storage.foldername(name))[1] = (select auth.uid())::text);

create policy "documents: update own" on storage.objects
  for update to authenticated
  using (bucket_id = 'client-documents'
         and (storage.foldername(name))[1] = (select auth.uid())::text)
  with check (bucket_id = 'client-documents'
```

```
              and (storage.foldername(name))[1] = (select auth.uid())::text);

create policy "documents: delete own" on storage.objects
  for delete to authenticated
  using (bucket_id = 'client-documents'
         and (storage.foldername(name))[1] = (select auth.uid())::text);
```

מה תוקן לעומת גרסאות נפוצות

- שם העמודה הוא file_size_limit. הנוסח max_file_size שמופיע בהדרכות רבות אינו קיים, והפקודה נכשלת.
- אין להמיר את שם התיקייה ל-uuid בתוך המדיניות. נתיב שאינו uuid זורק שגיאה ועלול להכשיל שאילתה שלמה. משווים בטקסט.
- כותבים (select auth.uid()) ולא auth.uid() ישירות, כדי שהערך יחושב פעם אחת בשאילתה.
- מדיניות UPDATE צריכה גם WITH CHECK, אחרת אפשר להעביר קובץ לתיקייה של אחר דרך שינוי שם.
- אל תתירו html או svg במאגר שנפתח בדפדפן בלי כותרת הורדה. קובץ כזה עלול להריץ סקריפט.

TPL-03 סריקת נוזקות לפני שמירה (תבנית לביצוע, לא פרוסה אצלנו)

הרעיון: הקובץ לא נכתב למאגר ישירות מהדפדפן. הוא עובר בפונקציית שרת, נבדק, ורק קובץ תקין נשמר. כרגע LALUM אינה סורקת נוזקות בקבצים שלקוח מעלה לפורטל, והם מגיעים ישירות למאגר פרטי עם מגבלת גודל ובלי סריקה.

- הזרימה: הלקוח שולח לפונקציה עם הטוקן שלו, הפונקציה מאמתת זהות, גודל וסוג, שולחת למנוע סריקה, ורק אחרי תשובה נקייה כותבת למאגר עם מפתח השירות, תחת תיקיית הבעלים. כדי שההעלאה הישירה לא תעקוף את הבדיקה, מסירים את מדיניות ה-INSERT של משתמשים מחוברים באותו מאגר.
- לקבצים גדולים אין להמתין סינכרונית. מעלים למאגר הסגר נעול, מנוע רקע סורק, וקובץ נקי מועבר למאגר היעד וקובץ נגוע נמחק עם התראה ורשומה ביומן. מאגר הסגר נעול (matter-quarantine) קיים במסד, ואין כרגע בקוד שימוש בו.

```
// Sketch of the gate. Not deployed in LALUM. SCANNER_URL is a ClamAV REST
// service that you operate, so the file never leaves your infrastructure.
const MAX_BYTES = 10 * 1024 * 1024;
const MAGIC: Record<string, number[]> = {
  "application/pdf": [0x25, 0x50, 0x44, 0x46],
  "image/png": [0x89, 0x50, 0x4e, 0x47],
  "image/jpeg": [0xff, 0xd8, 0xff],
};

class HttpError extends Error { constructor(public status: number) { super(String(status)); } }

async function cleanOrThrow(file: File): Promise<Uint8Array> {
  if (file.size > MAX_BYTES) throw new HttpError(413);
  const buf = new Uint8Array(await file.arrayBuffer());
  const sig = MAGIC[file.type];
  if (!sig || !sig.every((b, i) => buf[i] === b)) throw new HttpError(415); // the declared type must match
the bytes
  const r = await fetch(SCANNER_URL, { method: "POST", body: buf, signal: AbortSignal.timeout(20_000) });
  if (!r.ok) throw new HttpError(503);                // scanner down: fail closed, store nothing
  const verdict = await r.json();                     // { infected: boolean }
  if (verdict.infected !== false) throw new HttpError(422);
  return buf;
}
```

מה תוקן לעומת גרסאות נפוצות

- אין לשלוח מסמכים משפטיים לשירות סריקה ציבורי. לפי התיעוד של VirusTotal, קבצים שנשלחים אליו בשימוש הרגיל עשויים להיות משותפים מעבר לארגון שלכם, ורק מסלול Private Scanning בתשלום מחזיק אותם בתוך הארגון. לכן מנוע שאתם מפעילים בעצמכם (ClamAV) או בדיקה לפי גיבוב בלבד, בלי העלאה.
- סריקה שמחזירה סטטוס "בתור" מחזירה אפס זיהויים. קוד שקורא את התוצאה מיד ולא ממתין לסטטוס "הושלם" מעביר כל קובץ. נדרש polling עם תקרת זמן, וכשל סגור בתום התקרה.
- סוג הקובץ שהלקוח מצהיר עליו אינו ראיה. בודקים את הבתים הראשונים של הקובץ מול הסוג המוצהר.
- שם הקובץ מגיע מהלקוח. מנקים אותו או מייצרים שם בצד השרת, ואין להשתמש בו בנתיב כפי שהוא.
- תקלה במנוע הסריקה חייבת להיכשל סגור: הקובץ לא נשמר. פתיחה שקטה בכשל היא הדרך הנפוצה להפוך בקרה לקישוט.
- מגבלות גודל וזמן ריצה בפונקציית קצה חלות. מה שלא נכנס בהן הולך למסלול ההסגר.

https://docs.virustotal.com/docs/private-scanning

דיווח על חולשה

אם מצאתם חולשה או חשש אבטחה, פנו אל avraham@lalum.co. כתבו מה ראיתם, באיזו כתובת, ואיך אפשר לשחזר, ובלי לגשת למידע של אחרים או להשתמש בחולשה מעבר לנדרש כדי להדגים אותה.

פרטי הקשר מפורסמים גם בקובץ security.txt, בדרך המקובלת לכך.

העמוד מספק מידע כללי על בקרות אבטחה ואינו התחייבות חוזית ואינו ייעוץ משפטי. התחייבות כזו, אם תינתן, תיכתב בהסכם מול לקוח.