HPE Aruba Networking Central

נספח II: תיאור העיבוד

1.	תיאור העיבוד	השירות HPE Aruba Networking Central מעניק תפעול רשת מודרני ומקומי בענן והבטחת קישוריות לרשתות קוויות, רשתות Wi-Fi ורשתות SD-WAN. השירות HPE Aruba Networking Central משפר את יכולות הניהול המסורתיות הודות לרשת מבוססת בינה מלאכותית משולבת, תובנות ממשתמשים וניתוח פרופילים של רכיבי IoT להבטחת יכולות ניהול ושליטה אחודות ומאובטחות.
2.	סוג המידע האישי שמעובד	מידע אישי שנאסף כחלק מניהול הרשת ויישומים קשורים כולל: a. כתובת MAC של המכשיר b. כתובת IP של המכשיר c. מערכת הפעלה שמותקנת במכשיר d. שם המארח של המכשיר e. שם המשתמש f. כתובת דוא"ל (במקרה של רישום עצמי של אורח) g. מספר טלפון (במקרה של רישום עצמי של אורח) h. זהות ברשתות מדיה חברתית (במקרה של כניסת אורח באמצעות אישורי כניסה לרשת חברתית) i. שם תצוגה / חברות בקבוצה / תואם (במקרה של שימוש מורשה בענן)
3.	קטגוריות המידע האישי המעובד	לקוח הבקר, משתמש הקצה, עובד, עובד קבלן ועובד זמני.
4.	משך העיבוד	המידע שנאסף ומאוחסן במוצר הוא המידע המינימלי הנדרש כדי לעזור להבטיח גישה מאובטחת לפורטל וחיוני להבטחת הפונקציונליות שלו. כל יומני רישום הפעילות של המשתמש יימחקו באופן אוטומטי לצמיתות לאחר 90 יום.
5.	אמצעים טכניים וארגוניים	המעבד ישמור את המידע ויתחזק את תוכנית האבטחה הפיזית להגנה על המידע האישי של הבקר, כמפורט בנספח III להלן.

נספח III: אמצעים טכניים וארגוניים, כולל אמצעיים טכניים וארגוניים המיועדים להבטיח את אבטחת הנתונים

1. **מאפייני אבטחת מוצר:**

a. **אבטחה פיזית:** השירות HPE Aruba Networking Central מתארח בפלטפורמות IaaS עם שיעור האימוץ הנרחב ביותר – Amazon Web Services (AWS) ו-Microsoft Azure – שמציעות את תכונות האבטחה והתאימות המקיפות ביותר. הפלטפורמות AWS/Azure כוללות אמצעי אבטחה סביב האזורים הקריטיים ביותר, כולל האזור ההיקפי, התשתית, הנתונים ושכבות הסביבה.

b. **אבטחת רשת:** אבטחת הרשת של המעבד עוזרת לוודא שהרשת הפיזית והווירטואלית שבה שוכנים היישום והנתונים תמיד נותרת מאובטחת. המעבד משתמש בשירותים ובכלים שספקי IaaS מציעים, כמו גם בפתרונות צד שלישי מסוימים, כדי לוודא שסביבת הייצור של המעבד מאובטחת ככל האפשר מפני איומים חיצוניים ופגיעויות פנימיות. המעבד מפעיל מופעים נפרדים של הסביבות הפנימיות ושל סביבות הייצור. הסביבה הפנימית מתמקדת בפיתוח ובבדיקות, בעוד שסביבת הייצור שמורה אך ורק עבור הלקוחות שלנו (הבקר). ההפרדה הפיזית והלוגית של סביבת הייצור ממופעים אחרים שמופעלים עוזרת לנו להציע את האפשרות לפרוס תוכנה באופן המאובטח ביותר עבור לקוחותינו (הבקר) ולוודא שהנתונים שלהם תמיד מוגבלים לסביבה אחת.

c. **ארכיטקטורת ואבטחת היישום:** כל התעבורה בין היישום של Central והעולם החיצון מתבצעת באמצעות פתרון HTTPS over SSL. כל זרימת התעבורה מוצפנת באמצעות שימוש טכנולוגיית ההצפנה AES. שכבות יישומים שונות, כגון האינטרנט, יישומים ומסד הנתונים, נועדו לפעול תחת מסגרת של רשימת היתרים. רק נתיבי תקשורת הכרחיים ודרושים מורשים בין השכבות השונות. כל מופע בתוך השכבה מוגן באמצעות יישום כללי חומת אש, כדי למנוע גישה לא מורשית או זדונית.

d. **אבטחת נתונים:** כל מעבר הנתונים בין יישומים, מכשירים ומשתמשים מתרחש תוך שימוש בפתרון HTTPS. נתונים במנוחה מוצפנים ומאוחסנים. גיבוי נתונים מתבצע על בסיס שגרתי ומאוחסן עם יתירות. מנקודת מבט ארגונית, אנחנו מפעילים צוות DevOps שמנהל את כל היבטי האבטחה והתפעול של היישום.

e. **זמינות גאוגרפית:** HPE Aruba Networking Central זמין במדינות שונות ברחבי העולם כדי לאפשר לבקר לבחור באיזה אזור ליצור חשבון. גורמים שונים יכולים להשפיע על החלטה זו. למשל, ארגון עשוי לדרוש שכל הנתונים יישארו באזור מסוים או לכפות מגבלות רגולטוריות לגבי האופן שבו ניתן לעבד ולאחסן נתונים.

HPE Aruba Networking Central נפרס מאשכולות במרכזי נתונים נבחרים של Amazon Web Services (AWS) ו-Microsoft Azure, כשספקי שירותי הענן מספקים את תשתית המחשוב והאחסון. הטבלה הבאה כוללת פירוט של אשכולות HPE Aruba Networking Central ואזורים נתמכים:

אשכול HPE Aruba Networking Central	אזור AWS (העיר שבא נמצא האשכול)	הרשמה כתובת URL
US-1	us-west-2 (אורגון), US West	portal.central.arubanetworks.com/signup
US-2	us-west-2 (אורגון), US West	portal-prod2.central.arubanetworks.com/signup or console.greenlake.hpe.com
US-West-4	us-west-2 (אורגון), US West	portal-uswest4.central.arubanetworks.com/signup
US-West-5	us-west-2 (אורגון), US West	common.cloud.hpe.com
China-1	cn-north-1 (בייג'ינג), China	portal.central.arubanetworks.com.cn/signup
EU-1	eu-central-1 (פרנקפורט), EU	portal-eu.central.arubanetworks.com/signup
EU-Central2	eu-central-1 (פרנקפורט), EU	common.cloud.hpe.com
EU-Central3	eu-central-1 (פרנקפורט), EU	console.greenlake.hpe.com
Canada-1	Canada (Central), ca-central-1	portal-ca.central.arubanetworks.com/signup

אשכול HPE Aruba Networking Central	אזור AWS (העיר שבא נמצא האשכול)	הרשמה כתובת URL
APAC-1	Asia Pacific (מומבי), ap-south-1	portal-apac.central.arubanetworks.com/signup
APAC-East1	Asia Pacific (טוקיו), ap-northeast-1	portal-apaceast.central.arubanetworks.com/signup
APAC-South1	Asia Pacific (סידני), ap-southeast-2	console.greenlake.hpe.com

אשכול HPE Aruba Networking Central	אזור AWS (העיר שבא נמצא האשכול)	הרשמה כתובת URL
UAE North1	UAE North (דובאי)	common.cloud.hpe.com

כל הפעילות במכשירים שהוקצו לבקר תבוטל באשכול הנבחר, כולל נתונים סטטיסטיים של הרשת ונתוני טלמטריה שהועברו באמצעות חיבורי HTTPS. תצורת הנתונים עבור כל חשבונות הבקר נשמרת גם היא באשכול הנבחר.

כל הנתונים (כולל מידע אישי) שתואמים להתקני הרשת (כלומר, נקודות גישה, מתגים, שערים), מכשירי הבקר וכל נתוני משתמש אחרים מאוחסנים במסד נתונים באותו אשכול. כל עיבוד נוסף שעשוי להידרש מתבצע גם הוא במופעי מחשוב באותו אשכול או בהתאם ל-DPSA עבור שירותי המוצר HPE Aruba Networking.

— אמצעי אבטחה:

- המעבד ישמור את המידע הבא ויתחזק את תוכנית האבטחה הפיזית להגנה על המידע האישי של הבקר (להלן "תוכנית האבטחה של המעבד"):
  - התשתית של המעבד כוללת גרסאות עדכניות באופן סביר של תוכנת אבטחת המערכת, אשר עשויות לכלול חומת אש של המארח, הגנת אנטי-וירוס וכן תיקונים והגדרות וירוסים עדכניים. המעבד שומר על רישומים ביומן של אירועים שבהם מעורבת התשתית, כולל מערכות זיהוי חדירה המיועדות לצורך ניטור, זיהוי ודיווח על דפוסים של שימוש לרעה, פעילויות חשודות, משתמשים לא מאושרים וסיכוני אבטחה אחרים.
  - העובדים ועובדי הקבלן עברו הדרכה בנוגע למדיניות הפרטיות והאבטחה של המעבד והובהרו להם כל תחומי האחריות שלהם, בכל הנוגע לנוהלי הפרטיות והאבטחה. העובדים ועובדי הקבלן של המעבד מחויבים בחוזה לשמור על סודיות המידע האישי של הבקר ולציית למדיניות, לתקנים או לדרישות הרלוונטיים של המעבד בנוגע לעיבוד המידע האישי של הבקר. אי-ציות למדיניות, לתקנים או לדרישות אלה יהיה כפוף לחקירה שעשויה להוביל לענישה מנהלתית, עד וכולל סיום ההעסקה אצל המעבד או סיום ההתקשרות עם המעבד.
- אם הבקר מקבל מידע על תקרית אבטחה אשר משפיעה על השירותים, הבקר יודיע על כך למעבד בהקדם ועל היקף תקרית האבטחה. ההודעה תימסר באמצעות מרכז תפעול האבטחה של המעבד (Processor Security Operations Center) בדרך של שליחת הודעת דוא"ל אל הכתובת security@hpe.com.

שיחה בצ'אט עכשיו

בקר בכתובת HPE.com

© Copyright 2026 Hewlett Packard Enterprise Development LP. המידע המובא כאן כפוף לשינוי ללא הודעה מראש. האחריות היחידה המוגדרת עבור מוצרים ושירותים של Hewlett Packard Enterprise נכללת בהצהרות האחריות המפורשות, הנלוות למוצרים ולשירותים כגון אלה. אין לפרש דבר מתוך הדברים המובאים כאן כאחריות נוספת. Hewlett Packard Enterprise לא תהיה אחראית לכל שגיאות טכניות, שגיאות עריכה או להשמטות כלשהן במסמך זה.

Microsoft ו-Windows הנם סימנים מסחריים רשומים של Microsoft Corporation בארצות הברית ו/או במדינות אחרות. כל שאר הסימנים המסחריים של צדדים שלישיים הנם רכושם של בעליהם השונים בהתאמה.

a50009439HEE, מהדורה 3

HEWLETT PACKARD ENTERPRISE

hpe.com