

Pernyataan Keamanan

1. Tujuan

Pernyataan ini memberikan ringkasan publik atas praktik keamanan tertentu yang digunakan atau dimaksudkan untuk digunakan oleh PT UNIT GLOBAL SYSTEM untuk membantu melindungi Layanan, akun merchant, sistem teknis, dan Data Pribadi.

Pernyataan ini tidak menjelaskan seluruh sistem internal, konfigurasi, prosedur, kontrol, threshold, vendor, atau langkah keamanan.

2. Informasi Perusahaan

PT UNIT GLOBAL SYSTEM terdaftar di Republik Indonesia, NPWP 22.709.627.8-021.000, NIB 2511240128903, berkedudukan di Menara Cakrawala Lt. 12 Unit 05A, Jl. M.H. Thamrin, Kebon Sirih, Menteng, Kota Administrasi Jakarta Pusat, Provinsi DKI Jakarta, Jakarta, Kode Pos 10340, Republik Indonesia.

Laporan keamanan dapat dikirim ke security@unitpay.net.

3. Kontrol Akses

Perusahaan dapat menggunakan kontrol akses akun, izin berbasis peran, kontrol autentikasi, pembatasan akses personel, dan praktik tinjauan akses apabila sesuai.

Perusahaan dapat membatasi, menanggihkan, atau mengatur ulang akses apabila terdapat dugaan aktivitas mencurigakan, akses tidak sah, kompromi kredensial, atau penyalahgunaan.

4. Perlindungan Data

Perusahaan dapat menggunakan perlindungan teknis dan organisasi seperti enkripsi, transmisi aman, pembatasan akses, logging, prosedur backup, dan minimisasi data apabila sesuai dan tersedia.

Perlindungan dapat berbeda tergantung sistem terkait, jenis data, fitur layanan, pengaturan mitra, ketersediaan teknis, dan penilaian risiko.

5. Logging dan Monitoring

Perusahaan dapat menggunakan log, alert, tinjauan manual, pemberitahuan mitra, dan alat teknis yang tersedia untuk mengidentifikasi akses tidak sah, penyalahgunaan, masalah teknis, atau insiden keamanan.

Tinjauan keamanan dapat dilakukan berdasarkan peristiwa, secara berkala, manual, dipimpin mitra, atau didukung oleh alat teknis yang tersedia apabila sesuai.

6. Secure Development dan Vulnerability Management

Perusahaan dapat menerapkan praktik secure development, code review, dependency review, vulnerability remediation, dan pengujian teknis berdasarkan risiko, sumber daya yang tersedia, dan prioritas operasional.

Perusahaan dapat memprioritaskan remediation berdasarkan severity, exploitability, sistem terdampak, dampak pelanggan, persyaratan mitra, dan pertimbangan hukum atau regulasi.

7. Pelaporan Insiden

Merchant sebaiknya melaporkan dugaan akses tidak sah, kompromi kredensial, kompromi data, aktivitas API mencurigakan, atau insiden keamanan lain ke security@unitpay.net.

Perusahaan dapat meminta informasi tambahan, membatasi akses, merotasi kredensial, menyimpan log, memberi tahu pihak terkait, atau mengambil tindakan berbasis risiko lainnya apabila sesuai.

8. Tanggung Jawab Merchant

Merchant bertanggung jawab untuk melindungi sistem, kredensial, API keys, akses pengguna, data pelanggan, integrasi, perangkat, dan proses operasionalnya sendiri.

Merchant sebaiknya segera memberitahukan Perusahaan tentang dugaan kompromi, akses tidak sah, penyalahgunaan kredensial, atau masalah keamanan yang memengaruhi Layanan.

9. Kontak

Kontak keamanan: security@unitpay.net.