# Dasar Penggunaan Boleh Diterima

## 1. Gambaran Keseluruhan

Tujuan Dasar Penggunaan Boleh Diterima bukanlah untuk mengenakan sekatan yang bertentangan dengan K2 Bitumen Sdn. Bhd. (K2B) yang ditubuhkan dengan budaya keterbukaan, amanah dan integriti. K2B komited untuk melindungi pekerja, rakan kongsi dan Syarikat daripada tindakan yang menyalahi undang-undang atau merosakkan oleh individu, sama ada secara sedar atau tidak.

Sistem berkaitan internet atau intranet, termasuk tetapi tidak terhad kepada peralatan komputer, peranti mudah alih, perisian, sistem pengendalian, media storan, akaun rangkaian yang menyediakan e-mel, pelayaran WWW dan FTP adalah hak milik K2B. Sistem-sistem ini hendaklah digunakan untuk tujuan perniagaan bagi memenuhi kepentingan syarikat serta pelanggan dan klien kami semasa operasi biasa.

Keselamatan yang berkesan adalah usaha berpasukan yang melibatkan penyertaan dan sokongan setiap pekerja dan rakan sekutu K2B yang berurusan dengan maklumat dan/atau sistem maklumat. Adalah menjadi tanggungjawab setiap pengguna komputer untuk mengetahui garis panduan ini, dan menjalankan aktiviti mereka selaras dengannya.

## 2. Tujuan

Tujuan dasar ini adalah untuk menggariskan penggunaan yang dibenarkan bagi peralatan komputer dan peranti elektronik lain di K2B. Peraturan ini diwujudkan bagi melindungi pekerja dan K2B. Penggunaan yang tidak sesuai boleh mendedahkan K2B kepada risiko siber termasuk serangan virus seperti ransomware, kompromi sistem dan perkhidmatan rangkaian, kebocoran data, serta isu-isu perundangan.

## 3. Skop

Dasar ini terpakai kepada penggunaan maklumat, peranti elektronik dan pengkomputeran, serta sumber rangkaian untuk menjalankan urusan perniagaan K2B atau berinteraksi dengan rangkaian dalaman dan sistem perniagaan, sama ada dimiliki atau disewa oleh K2B, pekerja, atau pihak ketiga. Semua pekerja, kontraktor, perunding, pekerja sementara, dan pekerja lain di K2B serta anak syarikatnya bertanggungjawab untuk menggunakan pertimbangan yang wajar dalam penggunaan maklumat, peranti elektronik, dan sumber rangkaian selaras dengan dasar dan piawaian K2B, serta undang-undang dan peraturan Malaysia. Pengecualian terhadap dasar ini didokumenkan dalam seksyen 5.2.

Dasar ini terpakai kepada semua pekerja, kontraktor, perunding, pekerja sementara, dan lain-lain kakitangan di K2B, termasuk semua kakitangan yang bersekutu dengan pihak ketiga. Dasar ini juga terpakai kepada semua peralatan yang dimiliki atau disewa oleh K2B.

## 4. Polisi

### 4.1 Penggunaan dan Pemilikan Umum

***4.1.1*** Maklumat hak milik K2B yang disimpan dalam peranti elektronik dan pengkomputeran sama ada dimiliki atau disewa oleh K2B, pekerja atau pihak ketiga, kekal sebagai harta mutlak K2B. Anda mesti memastikan melalui kaedah perundangan atau teknikal bahawa maklumat hak milik ini dilindungi selaras dengan *Standard Perlindungan Data Peribadi Malaysia 2015.*

**4.1.2** Anda bertanggungjawab untuk segera melaporkan sebarang kecurian, kehilangan, atau pendedahan tanpa kebenaran terhadap maklumat hak milik K2B.

**4.1.3** Anda hanya boleh mengakses, menggunakan atau berkongsi maklumat hak milik K2B setakat yang dibenarkan dan diperlukan untuk melaksanakan tugas kerja yang telah diberikan kepada anda.

**4.1.4** Pekerja bertanggungjawab untuk menggunakan pertimbangan yang wajar berkenaan kesesuaian penggunaan peribadi. Setiap jabatan bertanggungjawab untuk menetapkan garis panduan berkaitan penggunaan peribadi sistem Internet atau Intranet. Sekiranya tiada dasar khusus ditetapkan, pekerja hendaklah merujuk kepada dasar jabatan mengenai penggunaan peribadi, dan sekiranya terdapat sebarang keraguan, pekerja perlu berunding dengan penyelia atau pengurus masing-masing.

**4.1.5** Bagi tujuan keselamatan dan penyelenggaraan rangkaian, individu yang diberi kuasa dalam K2B boleh memantau peralatan, sistem, dan trafik rangkaian pada bila-bila masa.

**4.1.6** K2B berhak untuk menjalankan audit ke atas rangkaian dan sistem secara berkala bagi memastikan pematuhan terhadap dasar ini.

### 4.2 Keselamatan dan Maklumat Hak Milik

**4.2.1** Semua peranti mudah alih dan pengkomputeran yang disambungkan ke rangkaian dalaman mesti mematuhi peraturan Akses Minimum, di mana prinsip hak akses minimum digunakan, iaitu pengguna hanya mempunyai akses kepada data dan sumber yang diperlukan untuk melaksanakan tugas harian mereka.

**4.2.2** Kata laluan pada peringkat sistem dan pengguna mesti mematuhi Dasar Perlindungan Kata Laluan. Memberikan akses kepada individu lain, sama ada secara sengaja atau akibat kegagalan untuk mengamankan akses tersebut, adalah dilarang.

**4.2.3** Semua peranti pengkomputeran mesti dilindungi dengan skrin kunci yang memerlukan kata laluan, dan fungsi pengaktifan automatik hendaklah ditetapkan kepada 10 minit atau kurang. Anda mesti mengunci skrin atau log keluar apabila peranti tidak digunakan atau ditinggalkan tanpa pengawasan.

**4.2.4** Sebarang hantaran oleh pekerja menggunakan alamat e-mel K2B ke kumpulan berita atau platform dalam talian lain hendaklah mengandungi penafian yang menyatakan bahawa pandangan yang dikemukakan adalah semata-mata pendapat peribadi mereka dan tidak semestinya mencerminkan pendirian K2B, kecuali jika hantaran tersebut dibuat sebagai sebahagian daripada tugasan kerja rasmi.

**4.2.5** Pekerja mesti berhati-hati sepenuhnya apabila membuka lampiran e-mel yang diterima daripada penghantar yang tidak dikenali, kerana ia mungkin mengandungi perisian hasad (malware).

## 4.3 Penggunaan yang Tidak Dibenarkan

Aktiviti-aktiviti berikut adalah secara umumnya dilarang. Walau bagaimanapun, pekerja boleh dikecualikan daripada sekatan ini sekiranya ia berkaitan dengan tanggungjawab kerja yang sah (contohnya: kakitangan pentadbiran sistem mungkin perlu menyahaktifkan akses rangkaian sesebuah hos sekiranya hos tersebut mengganggu perkhidmatan operasi).

Dalam apa jua keadaan sekalipun, pekerja K2B tidak dibenarkan terlibat dalam sebarang aktiviti yang menyalahi undang-undang tempatan, negeri, persekutuan atau undang-undang antarabangsa semasa menggunakan sumber milik K2B.

Senarai di bawah bukanlah senarai yang lengkap sepenuhnya, tetapi bertujuan untuk memberikan kerangka umum bagi aktiviti-aktiviti yang tergolong dalam kategori penggunaan yang tidak dibenarkan.

### 4.3.1 Aktiviti Sistem dan Rangkaian

Aktiviti-aktiviti berikut adalah dilarang sama sekali tanpa sebarang pengecualian:

1. Pelanggaran terhadap hak mana-mana individu atau syarikat yang dilindungi oleh undang-undang hak cipta, rahsia dagangan, paten atau harta intelek lain, atau undang-undang dan peraturan yang seumpamanya, termasuk tetapi tidak terhad kepada pemasangan atau pengedaran perisian "cetak rompak" atau produk perisian lain yang tidak dilesenkan dengan sah untuk digunakan oleh K2B.
2. Penyalinan bahan hak cipta tanpa kebenaran termasuk, tetapi tidak terhad kepada, pendigitalan dan pengedaran gambar dari majalah, buku atau sumber hak cipta lain, muzik hak cipta, serta pemasangan sebarang perisian hak cipta yang tidak mempunyai lesen aktif sama ada oleh K2B atau pengguna akhir adalah dilarang sama sekali.
3. Mengakses data, pelayan, atau akaun untuk sebarang tujuan selain daripada menjalankan urusan perniagaan K2B, walaupun anda mempunyai akses yang dibenarkan adalah dilarang.
4. Mengeksport perisian, maklumat teknikal, perisian penyulitan atau teknologi yang melanggar undang-undang kawalan eksport antarabangsa atau serantau adalah menyalahi undang-undang. Pihak pengurusan yang berkaitan hendaklah dirujuk terlebih dahulu sebelum mengeksport sebarang bahan yang diragui statusnya.
5. Pengenalan program hasad ke dalam rangkaian atau pelayan (contohnya: virus, worm, kuda trojan, ransomware dan sebagainya).
6. Mendedahkan kata laluan/frasa laluan akaun anda kepada orang lain atau membenarkan orang lain menggunakan akaun anda. Ini termasuk ahli keluarga dan penghuni rumah lain semasa kerja dilakukan di rumah.
7. Menggunakan aset pengkomputeran K2B untuk terlibat secara aktif dalam mendapatkan atau menghantar bahan yang melanggar undang-undang berkaitan gangguan seksual atau persekitaran kerja yang bermusuhan di bawah bidang kuasa tempatan pengguna.
8. Membuat tawaran palsu berkaitan produk, barangan atau perkhidmatan yang berasal daripada mana-mana akaun K2B.
9. Membuat kenyataan berkenaan jaminan, sama ada secara nyata atau tersirat, melainkan ia merupakan sebahagian daripada tugas kerja yang biasa.

10. Melakukan pelanggaran keselamatan atau gangguan terhadap komunikasi rangkaian. Pelanggaran keselamatan termasuk, tetapi tidak terhad kepada, mengakses data yang bukan ditujukan kepada pekerja atau log masuk ke pelayan atau akaun yang tidak diberi kebenaran secara jelas, kecuali jika tugas-tugas tersebut termasuk dalam skop kerja biasa. Bagi tujuan seksyen ini, "gangguan" termasuk, tetapi tidak terhad kepada network sniffing, ping floods, packet spoofing, serangan penafian perkhidmatan (denial of service), brute-force ke atas akaun, dan laluan pemalsuan maklumat untuk tujuan hasad.
11. Imbasan port atau imbasan keselamatan adalah dilarang sama sekali melainkan notifikasi awal telah diberikan kepada Pasukan Audit.
12. Melaksanakan sebarang bentuk pemantauan rangkaian yang memintas data yang tidak ditujukan kepada hos pekerja adalah dilarang, kecuali aktiviti tersebut merupakan sebahagian daripada tugas kerja rasmi pekerja.
13. Mengelakkan atau memintas pengesahan pengguna atau keselamatan mana-mana hos, rangkaian, atau akaun.
14. Memperkenalkan honeypot, honeynet, atau teknologi seumpamanya ke dalam rangkaian K2B adalah dilarang.
15. Mengganggu atau menafikan perkhidmatan kepada mana-mana pengguna selain hos pekerja sendiri (contohnya, serangan penafian perkhidmatan atau *denial of service attack*) adalah dilarang.
16. Menggunakan sebarang program/skrip/arahan, atau menghantar mesej dalam apa jua bentuk, dengan niat untuk mengganggu atau melumpuhkan sesi terminal pengguna, sama ada secara setempat atau melalui Internet atau Intranet adalah dilarang.
17. Memberikan maklumat mengenai, atau senarai nama pekerja K2B kepada pihak luar K2B adalah dilarang.

### 4.3.2 Aktiviti E-mel dan Komunikasi

Apabila menggunakan sumber syarikat untuk mengakses dan menggunakan Internet, pengguna mesti sedar bahawa mereka mewakili syarikat. Setiap kali pekerja menyatakan kaitan mereka dengan syarikat, mereka juga mesti dengan jelas menyatakan bahawa "pandangan yang dikemukakan adalah pandangan peribadi saya dan tidak semestinya mencerminkan pendirian syarikat" bagi ;

1. Menghantar mesej e-mel tanpa diminta, termasuk penghantaran "junk mail" atau bahan pengiklanan lain kepada individu yang tidak secara khusus meminta bahan tersebut (spam e-mel).
2. Sebarang bentuk gangguan melalui e-mel, telefon, mesej teks, atau sistem pemanggil (paging), sama ada melalui bahasa yang digunakan, kekerapan, atau saiz mesej.
3. Penggunaan tanpa kebenaran atau pemalsuan maklumat pengepala (header) e-mel.
4. Meminta e-mel bagi mana-mana alamat e-mel selain daripada akaun penghantar sendiri, dengan niat untuk mengganggu atau mengumpul balasan.
5. Mencipta atau memajukan "surat berantai", skim "Ponzi" atau skim "piramid" dalam apa jua bentuk.
6. Penggunaan e-mel tanpa diminta yang berasal daripada rangkaian K2B atau penyedia perkhidmatan Internet atau Intranet lain bagi pihak, atau untuk mengiklankan, sebarang perkhidmatan yang dihoskan oleh K2B atau disambungkan melalui rangkaian K2B.

7. Menyiarkan mesej yang sama atau hampir sama yang tidak berkaitan dengan urusan perniagaan ke sejumlah besar kumpulan berita Usenet (spam kumpulan berita).

### 4.3.3. Penulisan Blog dan Media Sosial

1. Aktiviti penulisan blog atau hantaran ke platform media sosial oleh pekerja, sama ada menggunakan harta dan sistem K2B atau sistem komputer peribadi, turut tertakluk kepada terma dan sekatan yang dinyatakan dalam Dasar ini. Penggunaan sistem K2B untuk tujuan penulisan blog atau hantaran dalam talian adalah tidak dibenarkan, dan penggunaan sistem komputer peribadi untuk blog atau media sosial juga tidak dibenarkan semasa waktu bekerja.
2. Dasar Maklumat Sulit K2B turut terpakai kepada aktiviti penulisan blog. Oleh itu, pekerja adalah dilarang mendedahkan sebarang maklumat sulit atau hak milik K2B, rahsia dagangan, atau apa-apa bahan lain yang dilindungi di bawah Dasar Maklumat Sulit K2B semasa menjalankan aktiviti penulisan blog.
3. Pekerja tidak dibenarkan terlibat dalam sebarang aktiviti penulisan blog yang boleh menjejaskan atau mencemarkan imej, reputasi dan/atau nama baik K2B dan/atau mana-mana pekerjanya. Pekerja juga dilarang daripada membuat sebarang komen yang bersifat diskriminasi, menghina, memfitnah atau mengganggu ketika menulis blog.
4. Pekerja juga tidak dibenarkan mengaitkan kenyataan, pendapat atau kepercayaan peribadi mereka dengan K2B semasa menjalankan aktiviti penulisan blog. Sekiranya pekerja menyatakan kepercayaan dan/atau pendapat mereka dalam blog, mereka tidak boleh secara nyata atau tersirat menggambarkan diri mereka sebagai pekerja atau wakil K2B. Pekerja menanggung sendiri segala risiko yang berkaitan dengan aktiviti penulisan blog.
5. Tanda dagangan, logo dan sebarang harta intelek lain milik K2B juga tidak boleh digunakan dalam apa-apa aktiviti penulisan blog atau media sosial.

## 5. Pematuhan Dasar

### 5.1 Pengukuran Pematuhan

**6.** Pasukan Audit akan mengesahkan pematuhan terhadap dasar ini melalui pelbagai kaedah, termasuk tetapi tidak terhad kepada, laporan alat perniagaan, audit dalaman dan luaran, serta maklum balas kepada pihak Pengurusan. Sebarang pengecualian terhadap dasar ini mesti mendapat kelulusan terlebih dahulu daripada Pasukan Audit.

### 6.1 Ketidakpatuhan

Pekerja yang didapati melanggar dasar ini boleh dikenakan tindakan disiplin, termasuk dan tidak terhad kepada penamatan pekerjaan.


Mohamed Nasser Bin Ahmad

Pengarah Urusan

05/05/2025

Rev. No. : 01