KEBIJAKAN YAYASAN PLAN INTERNATIONAL INDONESIA TENTANG (TEKNOLOGI INFORMASI KOMUNIKASI (ICT))

Tanggal Berlaku : Mei 2012
Tanggal Review : Mei 2013

Area Fungsional:	Teknologi Informasi dan Komunikasi	
Pemilik:	Kepala Petugas Informasi Global	
Disetujui oleh:	IH Executive – April 2012, POLT – Mei 2012	
Tanggal persetujuan:	9 Mei 2012	
Versi:	Final	
Tanggal tinjauan berikutnya:	Mei 2013	
Bahasa:	Inggris, Spanyol, Perancis	
Diberlakukan pada:	Plan International, Inc, kantor cabang dan anak perusahaan	
	Organisasi Nasional	TIDAK ADA Pedoman
Kontak:	Kepala Petugas Informasi Global – Mark Banbury	

Pendahuluan

Dokumen ini menguraikan kebijakan tentang penggunaan sistem Information and Communications Technology (ICT) (Teknologi Informasi dan Komunikasi (ICT)) Plan serta mencakup kebijakan berikut:

- Penggunaan Sistem Elektronik & Sistem Komputer Kebijakan Akses, Email, Kebijakan Penggunaan Internet Plan
- Kebijakan Kata Sandi
- Kebijakan penggunaan email
- Kebijakan ICT tentang staf yang keluar dari Plan; dan
- Kebijakan Akses Sistem untuk Staf Non-gaji/Non-Payroll.

Semua manajer di seluruh Plan Inc. bertanggung jawab untuk menerapkan kebijakan ini dan setiap anggota staf wajib mematuhinya.

Kebijakan ini akan ditinjau setiap tahun oleh Departemen Masyarakat dan Budaya serta ICT secara bersama-sama, dan diperbarui sesuai dengan praktik terbaik serta kebutuhan bisnis Plan.

Kebijakan ini tidak dimaksudkan untuk membatasi secara berlebihan, namun dirancang untuk memastikan bahwa sistem IT Plan aman dari akses yang tidak resmi.

1.1 PENGGUNAAN SISTEM ELEKTRONIK & SISTEM KOMPUTER PEDOMAN AKSES, EMAIL, PENGGUNAAN INTERNET PLAN

1.1.1 Tujuan

Plan telah melakukan investasi yang signifikan dalam pemasangan dan pemeliharaan sistem serta jaringan komputernya dengan akses ke email dan Internet untuk penggunaan organisasi guna meningkatkan efisiensi, efektivitas, dan produktivitas.

Untuk memastikan bahwa sistem komputer dan jaringan Plan digunakan demi keuntungan strategis Plan secara global dan bahwa risiko baik hukum atau dari kewajiban lain karena penggunaannya yang tidak tepat telah dikurangi, kebijakan global ini telah diperkenalkan ke semua pengguna sistem dan jaringan komputer Plan.

1.1.2 Cakupan

Kebijakan ini berlaku untuk semua pengguna sistem dan jaringan komputer Plan serta bagi siapa pun yang memiliki alamat Email Plan di mana pun mereka berada di dalam Plan Inc., termasuk di Kantor Negara, Kantor Regional, dan Kantor Pusat Internasional, salah satu kantorcabang mereka atau saat bekerja dari akses jarak jauh. Kebijakan-kebijakan ini merupakan pedoman bagi Organisasi Nasional dan direkomendasikan untuk adopsi modifikasi untuk inklusi kebijakan lokal.

Kebijakan ini mencakup penggunaan seluruh perangkat keras yang terhubung ke sistem milik Plan Inc., termasuk namun tidak terbatas pada desktop, laptop, netbook, ponsel, dan iPad (dan perangkat tablet lainnya) baik yang dimiliki oleh Plan atau tidak.

Sesuai dengan Pernyataan Tanggung Jawab, Kebijakan Standar di bawah ini dapat diadaptasi atau diperluas secara lokal sesuai dengan hukum setempat.

1.1.3 Pedoman Keseluruhan

Plan Inc. akan memberikan karyawan, dan dapat memberikan konsultan, kontraktor, mitra, dan sukarelawan, (disebut sebagai 'pengguna') akses elektronik penuh atau terbatas, tergantung pada peran mereka, ke sistem dan jaringan komputer Plan Inc. termasuk Email, Internet, Intranet, Extranet dan teknologi terkait lainnya. Plan akan memberikan pelatihan dan pendidikan yang relevan sesuai kebutuhan.

Plan mempromosikan penggunaan sistem dan jaringan komputernya untuk memfasilitasi komunikasi organisasi yang cepat, pembelajaran berkelanjutan, pengurangan pekerjaan kertas, dan kinerja pekerjaan yang efektif.

Plan melarang segala penggunaan sistem dan jaringan komputernya yang melanggar undang-undang atau kebijakan Plan yang berlaku, termasuk yang mencakup perlindungan anak, kesempatan yang sama, pelecehan ras dan seksual, diskriminasi, kerahasiaan, hak cipta dan hak milik, publikasi, intimidasi, perlindungan data, dan pribadi; dan/atau penggunaan apa pun yang berpotensi menyebabkan kerugian, risiko humas/risiko PR, kewajiban hukum atau lainnya terhadap Plan atau orang-orangnya.

Pelanggaran terhadap salah satu kebijakan oleh pengguna mana pun dapat mengakibatkan tindakan pendisiplinan termasuk pemutusan hubungan kerja atau hubungan kontrak/lainnya atau bahkan tuntutan pidana.

Seluruh pengguna harus mengetahui bahwa Plan dapat memblokir spam untuk mencegah kelebihan beban jaringan dan bahwa semua materi (termasuk Email) yang dibuat di sistem komputer Plan adalah milik Plan.

Tunduk pada hukum yang berlaku, Plan berhak untuk memantau, memeriksa, menyalin, meninjau, dan menyimpan kapan saja, tanpa pemberitahuan sebelumnya, salah satu dan semua hal berikut, sebagaimana diperlukan secara wajar untuk memastikan kepatuhan terhadap kebijakan ini: penggunaan (termasuk penggunaan pribadi sebagaimana diizinkan dalam kebijakan) sistem dan jaringan komputer Plan, termasuk akses ke Email dan Internet, serta setiap dan semua materi, file, informasi, perangkat lunak, komunikasi, dan konten lain yang dikirim, diterima, disimpan, atau dicetak sehubungan dengan penggunaan ini. (Disebut sebagai Pemantauan Penggunaan Sistem).

1.1.4 Pernyataan Tanggung Jawab

Setiap kantor Plan bertanggung jawab, (melalui CD, RD yang relevan atau, dalam hal IH, CIO Global, disebut sebagai Direktur Penanggung Jawab) dalam yurisdiksinya, untuk:

- Menerapkan dan menafsirkan kebijakan di lokasi masing-masing (di IH, ini merupakan tanggung jawab bersama CIO Global serta Direktur Masyarakat dan Budaya).
- Memelihara sistem dan jaringan komputer dengan keamanan yang memadai sesuai dengan konvensi yang ditentukan oleh tim Informasi dan Komunikasi (ICT) IH, dan memberikan pelatihan yang relevan kepada pengguna.
- Memelihara daftar alamat email, sesuai dengan konvensi yang ditentukan oleh IH ICT.
- Memastikan bahwa penolakan yang sesuai disertakan pada semua email eksternal yang dikirim oleh pengguna, sesuai dengan konvensi yang ditentukan oleh IH ICT. Untuk alasan hukum/bahasa dll., penolakan sebenarnya yang digunakan oleh setiap kantor/entitas Plan harus disesuaikan untuk memberikan nama resmi/nomor terdaftar/detail lainnya sebagaimana diwajibkan oleh hukum setempat.
- Memastikan penghentian segera akses pengguna ke sistem dan jaringan komputer Plan saat pengguna berhenti memiliki hubungan kontraktual dengan Plan.
- Menangani prosedur pendisiplinan di unit masing-masing (misalnya, di IH ini menjadi

tanggung jawab Direktur Masyarakat dan Budaya, bukan Global CIO).

- Memastikan kepatuhan dengan aturan penghapusan/retensi Email sebagaimana ditentukan oleh ICT lokal.
- Memastikan pelatihan dan pendidikan diberikan kepada pengguna akan kebijakan dengan berkonsultasi dengan Masyarakat dan Budaya.
- Memberikan persetujuan atau otorisasi yang diperlukan berdasarkan kebijakan ini.
- Pemantauan Penggunaan Sistem dalam yurisdiksi tersebut, sebagaimana ditentukan oleh Direktur Penanggung Jawab, asalkan semua pengguna di yurisdiksi tersebut diperlakukan sama.

***Catatan**: Kerahasiaan harus diperhatikan ketika dugaan pelanggaran terjadi, misalnya kunjungan yang jelas ke situs web porno. Terkadang hal ini tidak disengaja, atau materi dapat masuk ke komputer seseorang sebagai email yang tidak diminta. Pemeliharaan yang tepat harus diambil untuk melindungi kolega yang tidak bersalah. Pelatihan, pendidikan dan pembangunan kesadaran harus mendapat prioritas utama*

- Mencegah pengguna mengirim pesan apa pun dengan ukuran lebih besar dari 4 MB atau mengirim file kompresibel apa pun yang lebih besar dari 200KB tanpa zip.
- Memastikan bahwa pengguna menyimpan kata sandi mereka dengan aman dan mengubahnya seperlunya sesuai dengan kebijakan kata sandi Plan.
- Memastikan penerimaan tanda terima yang ditandatangani atas Kebijakan Akses Sistem Elektronik Plan dari setiap pengguna sebagaimana disajikan di bawah ini sesuai dengan hukum yang berlaku.

1.1.5 Kebijakan Standar: tunduk pada kepatuhan dengan Pernyataan Tanggung Jawab.

Kebijakan Standar		**Apa artinya ini bagi staf**
Para pengguna bebas untuk:		
1.	Akses email Plan, sistem komputer dan jaringan, kunjungi situs Internet dan gunakan alat Internet misalnya Instant Messenger kapan saja untuk keperluan terkait pekerjaan. Penggunaan pribadi	Untuk melindungi pengguna dari alat yang dapat membahayakan keamanan Plan (misalnya, infeksi virus) atau dapat menyebabkan kegagalan komputer karena ketidaksesuaian dengan teknologi kami

	diperbolehkan di luar jam kerja/jammakan siang asalkan tidak berlebihan dan tidak mengganggu kinerja pekerjaan. **Direktur Lokal dapat membatasi akses yang tidak terkait dengan pekerjaan kesistem karena kondisi lokal (ketersediaan bandwidth, konsumsi daya, dll.).**	yang ada, alat tidak boleh diunduh atau dipasang tanpa konsultasi dan persetujuan sebelumnya dari departemen IT. Permintaan harus diserahkan ke pendukung ICT lokal.
2.	Unduh/unggah file/perangkat lunak untuk kenyamanan terkait pekerjaan.	Untuk memastikan bahwa setiapperangkat lunak yang digunakan Plan telahdilisensikan dengan benar, dan untuk melindungi pengguna dari perangkat lunakyang dapat membahayakan keamanan Plan (misalnya infeksi virus) atau yang dapat menyebabkan kegagalan komputer karena ketidaksesuaian dengan teknologi kami yang ada; tidak ada perangkat lunak yang boleh diunduh atau dipasang tanpa konsultasi dan persetujuan sebelumnya oleh departemen ICT. Permintaan harus diserahkan ke tim pendukung ICT lokal. Mengunduh dokumen terkait pekerjaan dari situs terpercaya diperbolehkan.
Para pengguna dilarang untuk:		
1.	Mengirimkan informasi pribadi ataurahasia tentang sponsor, anak yang disponsori, pihak ketiga mana pun, Planatau pengguna lain mana pun kepada siapa pun, kecuali jika diperlukan sehubungan dengan pekerjaan Plan. (Jika informasi tersebut dikirim di luar jaringan email Plan, enkripsi yang tepat harus dipastikan dan persetujuan tertulis harus diperoleh dari individu/organisasi terkait sebagaimana diperlukan)	Staf harus memastikan bahwa informasi tersebut dienkripsi menggunakan file zip yang dilindungi kata sandi.
2.	Menelusuri atau melihat situs web yang berisi materi pornografi, menyinggung, atau berbahaya, dan/atau mengunduh, menampilkan, menyimpan, mencetak, mendistribusikan, atau mendistribusikan ulang materi semacam itu.	Cukup jelas
3.	Mengirimkan pesan apa pun yang menyembunyikan identitas pengirim. Mengirimkan atau meneruskan pesan	Email berantai dapat didefinisikan sebagai salah satu dari berikut ini: Email apa pun yang tidak terkait dengan

	berantai.	pekerjaan yang meminta Anda meneruskan pesan ke sejumlah orang. Email yang tidak diminta dikirim ke sejumlah orang, yang akan menganggapnya sebagai email sampah. Pesan-pesan ini dapat merusak sistem email saat pengguna meneruskan salinan ke lebih banyak orang.
4.	Memasang, tanpa izin resmi, di komputer Plan, perangkat lunak apa pun yang tidak dimiliki oleh Plan atau dilisensikan ke Plan; atau menggunakan perangkat lunak yang dimiliki atau dilisensikan oleh Plan di komputer non-Plan mana pun tanpa izin resmi.	Tidak ada perangkat lunak yang boleh dimuat tanpa konsultasi dan persetujuan sebelumnya oleh departemen ICT. Permintaan harus diserahkan ke tim pendukung ICT lokal. Pengunduhan dan pemasangan perangkat lunak screensaver dan webshots dilarang karena mengandung risiko tinggi infeksi virus dan dapat menyebabkan masalah komputer secara umum. Perangkat lunak yang dapat digunakan untuk mengunduh perangkat lunak ilegal dilarang. Pemasangan perangkat lunak yang dimiliki atau dilisensikan ke Plan di komputer non-Plan mana pun akan membatalkan lisensi dan karenanya dilarang.
5.	Menggunakan akun email eksternal untuk pekerjaan Plan, kecuali disetujui oleh kantor Plan lokal dan diproses oleh Global Helpdesk.	Penggunaan akun email eksternal untuk pekerjaan Plan hanya akan disetujui dalam keadaan darurat seperti: • Sistem email Plan gagal; atau • Ketidakmampuan untuk mengakses sistem email Plan saat bepergian. Akun email eksternal tidak boleh digunakan untuk mengirim informasi rahasia atau sensitif anak dalam keadaan apa pun. Sistem email Plan harus dapat diakses dari komputer mana pun dengan koneksi internet. Setiap masalah akses harus dilaporkan ke tim pendukung ICT lokal.
6.	Mengalihkan Email yang diterima di alamat Paket mereka secara otomatis ke akun email pribadi tanpa izin, kecuali pengaturannya diatur oleh Global Helpdesk.	Akun email eksternal tidak aman dan email yang dikirim secara eksternal dapat dibaca oleh sumber yang tidak sah. Pengguna Plan lain tidak akan mengetahui bahwa akun email Plan telah dialihkan ke akun

		eksternal dan mungkin secara tidak sengaja mengirimkan informasi rahasia ke akun eksternal. Untuk melindungi Anda dan Plan, pengalihan email yang dikirim ke akun Plan ke akun email eksternal dilarang.
Para pengguna harus:		
1.	Mengamankan kata sandi mereka danubah setidaknya sesering yang diminta oleh masing-masing kantor Plan. (Sistem dapat meminta ini jika memungkinkan.)	Kata sandi harus memenuhi persyaratan minimum yang ditentukan dalamKebijakan Kata Sandi IH.

1.1.6 Keamanan Sistem

Pada umumnya:

- Seluruh perangkat keras dan perangkat lunak komputer harus dipesan melalui dukungan ICT lokal.
- Sebagai titik awal dalam penyelidikan apa pun, Plan akan berasumsi bahwa Anda telah membuat semua materi yang tersimpan di cache komputer Anda. Oleh karena itu, Anda harus mengunci komputer jika Anda meninggalkan meja untuk waktu yang lama.

1.2 KEBIJAKAN KATA SANDI

Ketersediaan, integritas, dan kerahasiaan layanan dan informasi yang berkelanjutan yang disediakan oleh fasilitas teknologi komunikasi informasi Plan sangat penting untuk keberhasilan pengoperasian bisnis Plan. Potensi ancaman terhadap keamanan fasilitas inimengharuskan Plan untuk memastikannya memiliki kebijakan kata sandi yang sesuai. Rekomendasi yang dibuat oleh auditor eksternal kami dan standar industri saat ini digunakan sebagai dasar praktik terbaik dalam kebijakan ini.

1.2.1 Ruang Lingkup Kebijakan Kata Sandi

Kebijakan ini berlaku untuk:

- Semua karyawan, sukarelawan, pengawas, dan agen Plan;
- Karyawan, sukarelawan, dan agen dari organisasi lain yang mungkin memiliki akses ke dan/atau menggunakan sumber daya atau data ICT Plan.

1.2.2 Tujuan Kebijakan

Tujuan kebijakan adalah:

- Untuk melindungi data dan informasi Plan; Data dan informasi Plan akan dilindungi dari kehilangan, kerusakan, dan penyalahgunaan dari penggunaan yang tidak sah.
- Untuk memastikan kepatuhan staf dan sukarelawan terhadap prosedur kata sandi; Plan mewajibkan semua staf untuk mengetahui, dan mematuhi Prosedur kata sandi.

1.2.3 Tanggung Jawab atas Keamanan Kata Sandi

Staf

Setiap anggota staf bertanggung jawab untuk menjaga keamanan kata sandi dan tidak membocorkannya kepada pengguna lain.

Kata sandi bersifat individual karena suatu alasan; itu adalah praktik yang baik dan demi kepentingan terbaik Anda untuk menjaga kerahasiaan kata sandi Anda. Jika terjadi insiden dan dilacak kembali ke kata sandi Anda, asumsinya adalah Anda bertanggung jawab atas penyalahgunaan terkait sistem komputer.

Dalam keadaan luar biasa seperti staf sakit, tim pendukung ICT lokal dapat memberikan akses ke akun orang lain dengan menyetel ulang kata sandi. Permintaan seperti ini pertama-tama akan disetujui oleh manajer lini atau direktur departemen, dan ditandatangani oleh direktur terkait (seperti RD, CD, atau CIO Global).
Staf juga bertanggung jawab untuk memastikan bahwa kata sandi memenuhi persyaratan minimum berikut:

- Berisi karakter dari tiga dari empat kategori berikut:
  - Karakter huruf besar bahasa Inggris (A sampai Z),
  - Karakter huruf kecil bahasa Inggris (a sampai z),
  - Berbasis 10 digit (0 hingga 9),
  - Karakter non-alfanumerik (misalnya, !, $, #, %) dan,
- Panjangnya setidaknya delapan karakter;
- Diubah setidaknya setiap 90 hari;
- Tidak menggunakan kembali kata sandi lama.

Untuk lebih meningkatkan keamanan kata sandi tidak boleh:

- Berisi semua atau sebagian nama akun pengguna;
- Gunakan kata-kata (sederhana) yang mudah dikenali seperti ‘halo’ dan ‘selamat datang’;
- Gunakan kata sandi yang bersifat pribadi, seperti nama, tempat, warna atau tanggal lahir;
- Gunakan kata sandi yang serupa (yaitu, tidak boleh menyertakan amandemen kata sandi yang digunakan sebelumnya).

Tim ICT Global telah menerapkan mekanisme perangkat lunak untuk memastikan bahwa kerumitan kata sandi mengikuti aturan di atas dan bahwa kata sandi diperbarui setiap 90 hari.

Tim pendukung ICT lokal

Tim pendukung ICT lokal bertanggung jawab untuk menetapkan kontrol dan prosedur yang efektif untuk memastikan bahwa individu mematuhi persyaratan keamanan kata sandi minimum.
Karyawan yang bertanggung jawab membuat perjanjian dengan pengguna eksternal untuk penggunaan sumber daya pemrosesan informasi Plan harus mendapatkan persetujuan tertulis bahwa staf organisasi eksternal akan mematuhi kebijakan Plan saat menggunakan fasilitasnya.

1.3 KEBIJAKAN TENTANG PENGGUNAAN EMAIL DAN INTERNET

1.3.1 Penggunaan email secara umum

Dibandingkan dengan penulisan surat formal, email adalah bentuk komunikasi langsung dan dapat dianggap lebih informal. Namun, Anda harus berhati-hati (jika tidak lebih) dalam menyiapkan email seperti yang Anda lakukan saat menulis surat atau faks. Pernyataan yang tidak benar yang dikirim melalui email dapat menimbulkan tanggung jawab pribadi atau Plan, meskipun hanya dikirim secara internal. Selalu bekerja dengan asumsi bahwa pesan email dapat dibaca oleh orang lain selain penerima yang dituju, dan setelah ditulis email Anda dapat dianggap sebagai bagian dari catatan permanen.

Jangan mengirim email yang sepele atau tidak pantas (seperti surat berantai) dan hanya menyalin pesan ke orang yang perlu membacanya. Jika tidak, Anda akan berkompromi dengan

tujuan memiliki sistem, yaitu transfer informasi yang cepat dan efisien. Anda harus zip semua lampiran yang Anda kirim ke luar IH; alternatifnya, pertimbangkan untuk menyediakan lampiran berukuran besar di Intranet dan mengarahkan pengguna ke lokasi mereka melalui hyperlink.
Jika Anda mengirim email ke sekelompok besar individu, gunakan fungsi "BCC" untuk memasukkan alamat penerima, dan masukkan nama pengguna Anda sendiri di kolom. Mulai baris pertama email dengan penolakan yang menunjukkan siapa yang telah menerima email massal, seperti:

(Pesan berikut telah dikirim ke Direktur Nasional, Direktur Regional, Direktur Negara, Manajer NO dan RO ICT, Direktur Departemen IH dan Staf ICT IH)

Ini akan menghilangkan kemungkinan seseorang membalas Anda dan secara tidak sengaja menyalin seluruh grup. Jika Anda ingin orang lain menerima balasan, masukkan ke kolom "CC".
Anda harus segera melaporkan kepada tim pendukung ICT lokal setiap kejadian aktual, dugaan, atau ancaman yang Anda temui tentang email yang dicegat atau dirusak, atau dikirim atau diterima bertentangan dengan kebijakan yang tercantum di sini.

1.3.2 Penggunaan yang dilarang

Jangan pernah mengirim email yang kasar, seksis, rasis, diskriminatif, memfitnah, cabul, atau yang cenderung menyebabkan pelanggaran.

- Email yang kasar kemungkinan besar merupakan pelecehan, seperti email berulang dan tidak diinginkan yang meminta kencan, berisi sindiran atau komentar seksual, atau hanya mengganggu penerima tentang hal-hal yang tidak terkait denganpekerjaan. Yang penting adalah efek pada penerima, bukan apakah Anda berniatuntuk menyebabkan pelanggaran.
- Pertimbangan yang sama berlaku untuk masalah pelecehan ras.
- Pernyataan fitnah yang dikirim melalui email baik secara eksternal maupun internal dapat menyebabkan tanggung jawab hukum bagi Anda dan Plan, dan penggugat dapat mengajukan tindakan hukum di negara mana pun tempat pesan tersebut dibaca.

Plan mengakui bahwa tidak mungkin untuk mengontrol penerimaan oleh Anda atas materi yang menyinggung dari sumber eksternal; namun Anda bertanggung jawab untuk menyampaikan materi apa pun yang Anda terima kepada orang lain. Jika Anda menerima materi yang menyinggung, Anda harus memberi tahu supervisor Anda atau manajer lokal yangbertanggung jawab atas masyarakat dan budaya.
Silakan merujuk ke bagian Kebijakan Standar untuk perincian lebih lanjut.

1.3.3 Penggunaan Pribadi

Anda diizinkan untuk menangani urusan pribadi melalui email selama jam kerja, tetapi penggunaan pribadi ini tidak boleh berlebihan dan tidak boleh mengganggu kinerja pekerjaan Anda, juga tidak mengganggu kinerja sistem Plan. Akses ke penggunaan email pribadi mungkin dibatasi karena kendala ICT lokal. Anda tidak boleh menggunakan sistem untuk tujuan yang tidak pantas, misalnya untuk mengirim lelucon, kartun, atau surat berantai, atau untuk "Penggunaan yang dilarang" yang diuraikan di atas.
Silakan merujuk ke bagian Kebijakan Standar untuk perincian lebih lanjut.

1.3.4 Tanggung jawab karyawan untuk melindungi sistem Plan dari virus

Virus komputer menimbulkan ancaman yang signifikan terhadap stabilitas sistem ICT Plan dan merupakan tanggung jawab setiap pengguna untuk meminimalkan risiko pengenalannya.
Setiap email yang diterima dengan lampiran file non-teks (yang mungkin terdapat dalam lampiran file zip) harus dihapus kecuali secara jelas teridentifikasi berhubungan dengan pekerjaan. Jika Anda memiliki kecurigaan tentang lampiran file, khususnya lampiran non-teks, Anda harus merujuknya ke tim pendukung ICT lokal sebelum membukanya.

Setiap email yang Anda terima peringatan tentang potensi virus harus diteruskan ke tim pendukung ICT lokal, tidak diedarkan ke “semua orang”.

1.3.5 Kewajiban Hukum

Ingatlah selalu bahwa, saat Anda membuat email, Anda sedang membuat dokumen; mungkin diperlukan untuk diungkapkan dalam setiap proses Pengadilan, atau sebagai hasil dari penyelidikan yang dilakukan oleh pihak berwenang. Pesan email tidak secara otomatis dimusnahkan bahkan setelah ‘dihapus’ dan upaya untuk melakukannya bisa ilegal.

Anda harus berhati-hati untuk menghindari hubungan hukum atau komitmen kontraktual dengan pihak ketiga melalui email. Penting bagi Anda untuk tidak membuat pernyataan melalui email dalam negosiasi pra-kontrak yang tidak benar yang dapat menimbulkan klaim atas pernyataan yang salah, dan bahwa Anda tidak mencoba menyelesaikan kontrak melalui email.

Jangan pernah mengubah email orang lain dan meneruskannya tanpa menyorot perubahan Anda, karena ini bisa menjadi representasi yang keliru.

1.3.6 Pedoman penggunaan internet

Karyawan telah diberikan akses ke Internet sebagai alat untuk mendukung pekerjaan mereka. Penggunaan Internet sesekali untuk keperluan pribadi selama jam kerja diizinkan, asalkan tidak mengganggu kinerja pekerjaan Anda, dan disetujui bahwa hal tersebut tidak mengganggu jaringan dan sistem Plan (lihat bagian Kebijakan Standar). Namun, diharapkan karyawan pada umumnya akan membatasi penggunaan Internet untuk kepentingan pribadi di luar jam kerja. Anda tidak boleh menggunakan peralatan Plan kapan pun untuk mengakses situs ilegal, asusila, atau tidak pantas, khususnya situs dengan konten pornografi atau taruhan/perjudian online atau ruang obrolan online yang tidak terkait dengan bisnis Plan. Jika Anda masuk ke salah satu situs ini secara tidak sengaja, segera tinggalkan situs tersebut dan beri tahu manajer Anda.

Silakan merujuk ke bagian Kebijakan Standar untuk perincian lebih lanjut.

1.3.7 Pemantauan penggunaan email dan internet

Plan mengharuskan Anda untuk mematuhi pedoman yang diberikan dalam kebijakan ini dan, untuk memastikan kepatuhan terhadapnya dan mempertimbangkan apakah telah terjadi pelanggaran terhadapnya:

- Plan memiliki hak untuk memantau penggunaan email setiap karyawan secara individu termasuk volume email yang dikirim dan diterima, alamat email dikirim dari dan ke, dan deskripsi “subyek” di tajuk/header pesan. Jika ada alasan yang masuk akal untuk meyakini bahwa Anda telah melanggar kebijakan ini, Plan berhak memantau konten email, baik yang dikirim atau diterima sehubungan dengan pekerjaan Anda atau untuk alasan pribadi dan baik dikirim atau diterima selama atau di luar waktu jam kerja normal.

- Plan memiliki hak untuk memantau penggunaan Internet setiap karyawan secara individual termasuk volume dan waktu penggunaan Internet oleh setiap karyawan. Plan berhak memantau situs web yang telah dikunjungi dari sesi di mana nama pengguna Anda masuk; ini mungkin termasuk meninjau materi apa pun yang diunduh dari situs web menggunakan peralatan Plan (baik diakses dan/atau diunduh selama atau di luar jam kerja normal). Perlu Anda ketahui bahwa Plan mampu melacak seluruh riwayat situs Internet yang diakses oleh karyawan.

Dengan diterimanya kebijakan ini sebagai syarat pekerjaan Anda, Anda mengizinkan Plan untuk memantau penggunaan email dan Internet Anda dengan cara ini.

1.3.8 Peringatan pendisiplinan

Plan akan melakukan investigasi jika ada pengaduan penyalahgunaan sistem ICT (termasuk penyalahgunaan email dan/atau Internet), atau jika Plan mencurigai karyawan telah menyalahgunakan sistem tersebut. Plan secara tegas berhak mengakses perangkat karyawan yang disediakan oleh Plan (komputer, laptop, netbook, ponsel, tablet) untuk menyelidiki keluhan tersebut atau menyediakan perangkat karyawan yang disediakan oleh Plan kepada penasihat IT eksternal untuk melakukan penyelidikan yang diperlukan. Plan berhak menangguhkan Anda dari pekerjaan Anda untuk memungkinkan dilakukannya penyelidikan yang diperlukan.

Setiap penyalahgunaan sistem akan mengakibatkan tindakan pendisiplinan (hingga dan termasuk pemecatan singkat) terhadap Anda, sesuai dengan prosedur pendisiplinan Plan.

1.4 PEDOMAN ICT TENTANG STAF YANG KELUAR DARI PLAN

1.4.1 Pendahuluan

Plan berkepentingan untuk memastikan bahwa hanya staf saat ini yang dapat didaftarkan untuk menggunakan sistem dan peralatan komputer Plan, untuk menghindari potensi celah keamanan yang dapat digunakan untuk mengizinkan akses ke pengguna yang tidak berwenang, dan untuk melindungi kekayaan intelektual Plan.

Oleh karena itu, prosedur telah ditetapkan untuk memastikan kembalinya semua peralatan yang disediakan Plan dan untuk menghapus akun komputer dan alamat email staf ketika mereka meninggalkan organisasi.

Istilah “staf” dalam konteks ini terdiri dari staf gaji/payroll, konsultan, staf lembaga, dan sukarelawan. Staf didefinisikan sebagai pihak yang keluar/leavers ketika data keluar dimasukkan ke dalam sistem gaji/payroll. Untuk yang lainnya, tanggal keluar akan ditetapkan saat akun komputer mereka dibuat.

1.4.2 Rekening Gaji/Payroll Staf

Sebelum seorang anggota staf keluar dari Plan, semua file di dalam filestorenya yang perlu disimpan harus dipindahkan ke filestore anggota staf lain yang akan mengambil alih tanggung jawab yang keluar. Ini adalah tanggung jawab bersama dari pihak yang keluar/leaver dan administrator kantor/departemen. Sama halnya, adalah tanggung jawab pihak yang keluar/leaver untuk menghapus sebelum dia meninggalkan file pribadi dan rahasia yang dia tidak ingin diakses oleh orang lain. Pihak yang keluar/Leavers juga bertanggung jawab untuk menghapus nama mereka dari milis elektronik mana pun yang telah mereka langgan.

- Staf yang berhenti bekerja di Plan diingatkan bahwa setiap perangkat lunak komputer yang dipasang berdasarkan Lisensi Program pada komputer yang tidak dimiliki Plan (misalnya IPASS, produk Microsoft Office, dll., yang dilisensikan berdasarkan Perjanjian Program) HARUS dihapus. Kegagalan untuk mengambil tindakan akan menganggap perangkat lunak tersebut tidak berlisensi dan karenanya ilegal.
- Akun dan filestore Pihak yang keluar/Leaver akan dihapus satu bulan setelah tanggal keberangkatan mereka. Manajer lini pihak yang keluar/leaver/kepala departemen bertanggung jawab untuk menerapkan prosedur pengecualian untuk setiap staf yang pendaftaran dan penyimpanan filenya perlu dipertahankan.
- Prosedur ini dirancang untuk mengakomodasi staf yang terus bekerja sama dengan Plan dalam kapasitas paruh waktu setelah mereka pergi. Mereka tidak boleh disalahgunakan untuk meniadakan proses keamanan.
- Jika ada anggota staf yang keluar tanpa pemberitahuan (misalnya karena kematian dalam pelayanan), administrator kantor/departemen akan bertanggung jawab untuk memulai transfer file ke akun alternatif sebelum akun asli dihapus.
- Prosedur pengecualian untuk pihak yang keluar/leaver dengan alasan yang sah untuk mempertahankan akun mereka akan dimulai setelah menerima otorisasi resmi dari manajer lini/kepala departemen mereka dan disetujui oleh direktur terkait (RD, CD, Global CIO). Prosedur ini harus diserahkan ke Helpdesk dalam periode satu bulan setelah tanggal keluar; prosedur tersebut harus menentukan periode retensi (maksimal 12 bulan) untuk perpanjangan pendaftaran mereka. Pada akhir periode perpanjangan yang ditentukan, pendaftaran dan penyimpanan file yang keluar akan dihapus secara otomatis kecuali otorisasi lebih lanjut telah diterima untuk sementara. Staf non-payroll akan diperlakukan dengan cara yang sama seperti pihak yang keluar/leaver, artinya mereka akan diizinkan untuk mempertahankan akun mereka hanya atas permintaan tegas dari manajer lini/kepala departemen mereka. Permintaan ini perlu diperbarui setiap tahun.
- Satu bulan setelah anggota staf keluar, jika prosedur pengecualian tidak diterapkan, ICT lokal akan menghapus pendaftaran pihak yang keluar/leaver di komputer pusat dan menghapus semua file data dan pesan surat elektronik di penyimpanan file pihak yang keluar/leaver di komputer tersebut. Semua kantor/Departemen harus mencatat bahwa permintaan untuk memulihkan file harus diterima dalam waktu 2 minggu sejak tanggal penghapusan.
- Administrator kantor/departemen bertanggung jawab untuk menetapkan aturan balasan dan penerusan pada akun email pihak yang keluar/leaver pada tanggal keberangkatan mereka. Aturan balasan harus menjelaskan bahwa penerima telah meninggalkan organisasi dan email diteruskan ke kontak yang ditunjuk. Aturan penerusan harus meneruskan email ke administrator departemen atau kontak yang ditunjuk. Surat tidak boleh diteruskan ke alamat email eksternal pihak yang meninggalkan.
- Setiap administrator kantor/departemen bertanggung jawab untuk memberitahukan ICT lokal mereka ketika seorang karyawan akan cuti. Hal ini dapat dilakukan melalui Global Helpdesk dengan melengkapi formulir pihak yang keluar/leaver di **pla**net.

- ICT lokal bertanggung jawab untuk mencabut akses para pihak yang keluar/leaver ke sistem Plan pada tanggal keberangkatan dan menghapus semua file data dan pesan surat elektronik di penyimpanan berkas para pihak yang keluar/leaver baik satu bulan setelah keberangkatan atau pada tanggal yang ditentukan oleh orang yang meminta prosedur pengecualian.

1.4.3 Seluruh rekening lainnya

- Sebelum anggota staf non-payroll keluar dari Plan, file di penyimpanan filenya, yang perlu disimpan untuk keperluan penelitian atau administratif yang sedang berlangsung, akan ditransfer ke akun yang sesuai. Demikian juga, ini adalah tanggung jawab staf non-payroll untuk menghapus sebelum dia meninggalkan file pribadi dan rahasia yang dia tidak ingin diakses oleh orang lain. Pihak yang keluar/Leavers juga bertanggung jawab untuk menghapus nama mereka dari milis elektronik mana pun yang telah mereka langgan.
- Staf ini tidak akan diberi pemberitahuan tentang penghapusan akun dan penyimpanan file mereka.

1.4.4 Peralatan pihak yang keluar/leaver dan peralatan yang tidak biasa digunakan

- Sebelum seorang anggota staf meninggalkan Plan, manajer lini/administrator departemen pihak yang keluar harus memastikan bahwa semua peralatan yang disediakan oleh Plan telah dialihkan ke anggota staf lain yang akan mengambil alih tanggung jawab pihak yang keluar, atau dikembalikan, seperti di bawah ini.
- Mengembalikan ke ICT seluruh peralatan komputer yang mungkin memiliki data Perusahaan di dalamnya, atau mungkin terhubung ke jaringan dengan cara apa pun yang tidak digunakan secara rutin dan ditugaskan kepada karyawan Plan.
- Peralatan ini akan dibersihkan datanya dan dijadikan Stok Pinjaman, atau dibuang dengan aman, dan selanjutnya **tidak lagi menjadi risiko keamanan karena kurangnya penyimpanan yang aman atau pembaruan antivirus otomatis**. Ini berlaku terutama untuk komputer laptop.

Semua peralatan komputer cadangan atau pinjaman harus dikembalikan ke ICT saat tidak digunakan. Hanya Departemen ICT yang diperbolehkan menyimpan peralatan komputer cadangan atau pinjaman.

1.5 AKSES SISTEM BAGI STAF NON-PAYROLL

1.5.1 Pendahuluan

Setiap anggota staf, staf sementara, kontraktor, konsultan, sukarelawan, atau perwakilan lain dari Plan yang menggunakan sistem ICT Plan, harus mematuhi kebijakan ini.

Di seluruh kebijakan ini, istilah “staf non-gaji/staf non-payroll” berlaku untuk staf sementara, sukarelawan, konsultan & kontraktor yang tidak termasuk dalam sistem payroll Plan.

1.5.2 Kebijakan

Plan secara teratur mempekerjakan staf non-gaji/non-payroll dalam menjalankan bisnisnya. Penting agar sistem ICT Plan diamankan dari akses tidak sah sambil memastikan bahwa staf non-gaji/non-payroll memiliki akses yang memadai untuk menjalankan peran mereka selama jangka waktu kontrak mereka.

Staf non-gaji/non-payroll harus mematuhi seluruh kebijakan Plan dan kebijakan yang meliputi Penggunaan & Akses ke Internet, dan Email & Sistem Komputer Plan.

Mematuhi kebijakan ini akan memungkinkan staf non-gaji/ non-payroll untuk menjalankan peran mereka secara efektif tanpa mengorbankan sistem ICT Plan dan akan mengurangi risiko akses tanpa izin.

1.5.3 Akses ke Sistem Plan

Akses ke sistem ICT Plan hanya akan diberikan kepada staf non-gaji/non-payroll yang memerlukan akses ke sistem Plan untuk menjalankan peran mereka. Semua permintaan akses ke sistem Plan harus diajukan ke dukungan ICT lokal, yang akan membuat akun yang memberikan tingkat akses yang sesuai untuk peran mereka kepada anggota staf non-gaji/non-payroll.

Manajer lini anggota non-gaji/non-payroll bertanggung jawab untuk mengirimkan permintaan ke dukungan ICT lokal. Permintaan harus menyertakan:

- Nama lengkap orang tersebut, nama perusahaan (jika ada) dan posisinya
- Daftar sistem yang mereka butuhkan aksesnya (termasuk email jika diperlukan)
- Tingkat akses yang diperlukan untuk setiap sistem; dan
- Tanggal mulai dan berakhir kontrak (tanggal kedaluwarsa akun)

Dukungan ICT lokal bertanggung jawab untuk membuat dan menghapus akun. Akun akan dinonaktifkan pada tanggal kedaluwarsa yang ditentukan pada permintaan, dan dihapus sesuai kebijakan Plan tentang penghapusan akun komputer.

Staf sementara, kontraktor, dan sukarelawan diizinkan menggunakan akun email Plan untuk menjalankan peran mereka. Konsultan tidak diizinkan menggunakan akun email Plan.

Kebijakan ini telah dilihat dan disetujui oleh:

Nigel Chapman (tanda tangan):_____Tanggal:_____

Chief Executive Officer, Plan International, Inc

KEBIJAKAN ICT BAGI PARA PENGGUNA

KEBIJAKAN ICT UNTUK PENGGUNA

Pengesahan

Saya memahami ketentuan Kebijakan ICT Plan untuk Pengguna dan setuju untuk mematuhinya. Saya setuju bahwa Plan dapat memantau pesan email yang saya kirim dan terima, aktivitas saya yang terkait dengan akses Internet, dan aktivitas sistem apa pun termasuk pengiriman atau penerimaan file apa pun. Saya memahami bahwa setiap pelanggaran terhadap kebijakan mana pun dapat mengakibatkan tindakan pendisiplinan termasuk pemutusan hubungan kerja (atau hubungan kontrak/lainnya) atau bahkan tuntutan pidana.

Tanda tangan: _____

Nama: _____

Posisi: _____

Lokasi: _____

Tanggal: _____