Para sa mga SME at mga namamahala ng maliliit na negosyo

Limang Minutong Pansariling Ebaluwasyon ng Kompanya sa Seguridad ng Impormasyon

Alam mo ba ang mga nauuso ngayon?

Mga umuusbong na mga panganib at mga pag-atake

- Ransomware
- Mga pag-atake sa nakatalang password
- Mga pinuntiryang pag-atake sa email

Mga pagbabago sa mundo ng IT

- Ang Cloud
- Mga tablet
- Mga smartphone

Gamitin ang **"Talaan para sa Limang Minutong Pansariling Ebaluwasyon ng Kompanya"** nang masuri ang estado ng seguridad nito bago mawala ang mga datos!

ASEAN · JAPAN
Cybersecurity Cooperation

Pansariling Ebaluwasyon

1 Mangyaring basahin ito bago isagawa ang ebaluwasyon.

Paano gamitin

Itinuon namin ang atensyon sa dalawampu't limang epektibong gawain ukol sa seguridad ng impormasyon na maaari ring ipatupad nang may maliit lamang na gastos sa kompanya.
Mangyaring suriin ang estado ng implementasyon ng mga ito at ipatupad ang mga gawaing hindi pa naisasagawa habang sumasangguni sa mga pagpapaliwanag sa pulyetong ito.

Layunin at mga pakinabang

- Tutulungan ka nitong maintindihan ang mga problemang maaaring mangyari.
- Sa pamamagitan ng pag-intindi sa mga problema, malalaman mo ang tiyak na aksyon bilang sunod na hakbang.

Paano basahin ang mga deskripsyon

Mangyaring magpasya nang hindi umaasa sa mga natukoy na halimbawa sa mga deskripsyon. Halimbawa, ang tinutukoy sa ikalabing-anim na tanong ay tungkol sa "mga gawain upang maiwasan ang pagnanakaw." Itinatanong nito kung nagsagawa ka ng mga hakbang upang maiwasan ang pagnanakaw sa pamamagitan ng paglalagay ng mga laptop sa drawer kung ang organisasyon ay gumamit nito. Itinatanong rin nito kung nagsagawa ka ng mga hakbang upang maiwasan ang pagnanakaw sa pamamagitan nang hindi pag-iwan sa mga kagamitan tulad ng mga USB stick o external hard drive sa mga lamesa kung ang iyong organisasyon ay walang mga laptop. Sumangguni sa pulyeto kung hindi mo naintindihan ang layunin ng katanungan o kung nahihirapan kang intindihin ito.

Kung ang iyong kompanya ay walang ginagamit na bagay

Maaaring hindi puwede sa iyong kompanya ang ilang mga bagay sa ibaba depende sa uri ng negosyo. Sa mga pagkakataong ito, bilugan ang "Naipatupad."

- Bilang 4 Mga copier at hard drive na nakakonekta sa network
- Bilang 5 Mga serbisyo sa Web
- Bilang 9 Mga wireless LAN
- Bilang 23 Mga serbisyo sa Cloud

Kung iniisip mong "Wala kaming kahit anong 'kumpidensyal na impormasyon', ang mga bagay sa ibaba ay mga kumpidensyal na mga materyal!

- Lugar ng tirahan ng mga empleyado, at mga pay slip
- Listahan ng mga binayaran sa bawat kasosyo sa negosyo at impormasyon ng transaksyon
- Impormasyon sa accounting ng iyong organisasyon
- Mga listahan ng kontak ng mga kliyente at kasosyo sa negosyo
- Impormasyon sa progreso gaya ng disenyo ng mga guhit para sa mga bagong produkto
- Kahit anong impormasyon mula sa mga kasosyo sa negosyo na kailangang ingatan nang mabuti

Mayroong impormasyon na kailangang pamahalaan bilang kumpidensyal sa lupon ng mga pangunahing impormasyon ng isang organisasyon. Kailangan mong kumpirmahin at iorganisa kung anong uri ng kumpidensyal na impormasyon ang mayroon sa iyong kompanya. Ang pag-uuri ng mga datos ang unang hakbang sa seguridad ng impormasyon.

2 Mangyaring sagutan ang dalawampu't limang tanong sa talaan ng Pansariling Ebaluwasyon ng Kompanya.

Kung nakakuha ka ng 100 puntos	Perpekto na ang iyong pangunahing mga hakbang sa seguridad. Pag-isipan mo ang pagpapahusay pa ng mga hakbang na ito.
Kung nakakuha ka ng 70-99 na puntos	Halos perpekto na subalit may ilang mga bahagi na may kakulangan sa mga hakbang.
Kung nakakuha ka ng 50-69 na puntos	Mayroong kapansin-pansing mga bahagi na may kakulangan sa mga hakbang.
Kung nakakuha ka ng 49 na puntos o mas mababa	Hindi ka dapat magulat kung mayroong insidente tulad ng paglabas ng lihim na mga datos.

Ang mga hakbang na isinalarawan sa talaan ng Pansariling Ebaluwasyon ng Kompanya ay nakabase sa mga sumusunod.

- Maaaring direktang turuan o kumpirmahin ng tagapagpaganap (representante) kung ang mga hakbang sa polisiya ay naipapatupad.
- Kinikilala ng lahat ng mga empleyado ang bawat isa.
- Hindi nagmamay-ari ng server o kagamitan sa network ang kompanya na nangangailangan ng komplikadong mga setting.
  - Hindi gumagamit ng server ang website ng kompanya na direktang konektado sa Internet, gaya ng paggamit ng serbisyo na pang-cloud.
  - Walang nagawang application software ang kompanya, at gumagamit lamang ito nang nabibiling application software.
  - Maaari lamang gamitin ang mga personal computer para sa trabaho kung ang ipinapatupad na mga hakbang ay kapareho para sa mga computer na pagmamay-ari ng kompanya.

Pansariling Ebaluwasyon

Talaan ng Limang Minutong Pansariling Ebaluwasyon ng Kompanya

Talaan ng pansariling ebaluwasyon ng kompanya upang matukoy ang mga hakbang para sa seguridad ng impormasyon na kailangang bigyan ng priyoridad bilang isang organisasyon.

- Mangyaring basahin ang 1 sa naunang pahina bago isagawa ang ebaluwasyon.
- Basahin ang mga bagay kaugnay ng ebaluwasyon sa ibaba at bilugan ang hanay na naaangkop.
- Kailangang punan ang talaang ito ng mga tagapagpaganap o tagapagpamahala.
- Mangyaring sagutan kung ang natukoy na mga bagay ay naisasagawa ng lahat ng mga empleyado. Kung ito ay naisasagawa ng ilang mga empleyado lamang, piliin ang “bahagyang naipatupad.”
- Mangyaring sagutan kung ang natukoy na mga bagay ay naipatutupad ng iyong kompanya.
- Bilangin ang iyong puntos sa ibaba ng pahina, at magpatuloy sa pagbabasa ng 2 sa naunang pahina.

Organisasyon: _____

Respondente: _____

Petsa: _____

Bagay na sinusuri	Bilang	Deskripsyon	Tugon			
			Naipatupad	Bahagyang naipatupad	Hindi naipatupad	Hindi alam
Unang Bahagi Pangunahing mga hakbang	1	Pinananatili mo bang protektado ang iyong OS at software sa pamamagitan ng pag-update ng Windows (Windows Update)*1 o sa pamamagitan ng ibang mga hakbang?	4	2	0	0
	2	Nagsasagawa ka ba ng mga hakbang upang protektahan ang iyong PC laban sa mga virus, tulad ng pag-install ng antivirus software at awtomatikong pag-update ng mga virus definition file?*2	4	2	0	0
	3	Nag-set ka ba ng password na hindi madaling mahulaan at hindi ka ba gumamit ng mga password tulad ng iyong pangalan, numero ng telepono, o petsa ng kaarawan, at iniiwasan mo bang gumamit ng parehong password para sa iba't-ibang mga serbisyo sa web?	4	2	0	0
	4	Angkop mo bang nililimitahan ang akseso sa mahalagang impormasyon, tulad ng paglimita sa pagbabahagi ng mga copier o hard drive na konektado sa network para lamang sa mga taong nangangailangan nito?	4	2	0	0
	5	Mayroon bang umiiral na sistema na iyong ginagamit upang matukoy ang bagong panganib at paraan ng pag-atake at internal na maibahagi ito sa pamamagitan ng pagsuri at pagbahagi ng mga alertong panseguridad mula sa mga gumagawa ng produkto o mga serbisyo sa web*3?	4	2	0	0
Ikalawang Bahagi Mga hakbang bilang isang empleyado	6	Nag-iingat ka ba sa pagkalap ng mga email, at sinisigurado mo bang hindi magbukas ng bagay na kalakip ng kahina-hinalang mga email o mga click link sa mga mensahe?	4	2	0	0
	7	Mayroon bang umiiral na sistema upang masuri at maiwasan ang maling pagpapadala ng mga e-mail, tulad ng biswal na pagsusuri ng mga e-mail address bago ito ipadala?	4	2	0	0
	8	Pinuprotektahan mo ba ang mahalagang impormasyon sa pamamagitan ng paglalagay ng password sa mga kalakip na bagay o iba pang kaparehong hakbang bago magpadala ng mga email?	4	2	0	0
	9	Nasasagawa ka ba ng mga hakbang upang ingatan ang iyong mga wireless LAN, tulad ng palagiang pagpapatupad ng malakas na encryption kapag ginagamit ang mga ito?	4	2	0	0
	10	Nagsasagawa ka ba ng mga hakbang upang makontrol ang paggamit ng Internet, tulad ng pag-set ng mga panuntunan sa pagbisita sa mga website at pag-post sa social media gamit ang mga computer sa opisina?	4	2	0	0
	11	Nagsasagawa ka ba ng mga hakbang para sa regular na mga pag-backup upang maiwasan ang pagkawala ng mahahalagang impormasyon dulot ng mga pagpalya o kamalian sa operasyon?	4	2	0	0
	12	Nagsasagawa ka ba ng mga hakbang upang maiwasan ang pagkawala o paglabas ng mahalagang impormasyon, tulad ng paglalagay ng mga ito sa isang nakasarang cabinet sa halip na iwanan ito sa lamesa?	4	2	0	0
	13	Kapag naglalabas ng mahalagang impormasyon mula sa opisina, nagsasagawa ka ba ng mga hakbang laban sa pagnanakaw o pagkawala, tulad ng pagprotekta nito sa pamamagitan ng paglalagay ng password o pag-encrypt at pagsigurado na nasa iyo ito lahat ng oras?	4	2	0	0
	14	Nagsasagawa ka ba ng mga hakbang upang masigurado na hindi nagagamit ng iba ang iyong computer, tulad ng pag-set ng lock screen ng computer kapag ikaw ay umaalis sa iyong lamesa?	4	2	0	0
	15	Sinusubukan mo bang iwasan ang hindi awtorisadong mga tao na makapasok sa opisina sa pamamagitan ng pagkikipag-usap sa mga hindi kakilala kapag napansin mong may taong hindi pamilyar o sa pamamagitan ng ibang mga hakbang?	4	2	0	0
	16	Nagsasagawa ka ba ng mga hakbang upang maiwasan ang pagnanakaw kapag umaalis sa opisina sa buong araw, tulad ng pagsara ng mga laptop at mga kagamitan sa drawer sa halip na iwanan lamang ang mga ito sa lamesa?	4	2	0	0
	17	Maayos bang pinamamahalaan ang mga susi sa opisina, tulad ng pagsara nito ng kung sino mang huling umalis sa araw na iyon at pagtatala nito (kasama ang kanilang mga pangalan, petsa, at oras)?	4	2	0	0
	18	Kapag nagtatapon ng mahalagang impormasyon, nagsasagawa ka ba ng mga hakbang upang hindi na ito mababasa, tulad ng pagpira-piraso ng mga dokumento o paggamit ng kagamitan sa pagbura ng mga datos?	4	2	0	0
Ikatlong Bahagi Mga hakbang bilang isang organisasyon	19	Mayroon ka ba sa iyong Lipon ng Alituntunin sa Pagkilos ng Empleyado na may kinalaman sa kumpidensyalidad, tulad ng pagpapaalam sa mga empleyado kung sila ay natanggap sa trabaho at sila ay obligadong panatilihin itong kumpidensyal at mayroong mga probisyon sa parusa?	4	2	0	0
	20	Ikaw ba ay nagsasagawa ng kasanayan sa pagbatid ng seguridad upang malaman ng mga empleyado ang kahalagahan ng pamamahala sa impormasyon, tulad ng regular na pagpapaliwanag ng importansya nito?	4	2	0	0
	21	Inalam mo ba nang klaro kung ang mga empleyado ay maaaring gumamit ng personal na mga device sa kanilang trabaho, tulad ng pag-set ng mga polisiya sa paggamit ng mga personal computer at smartphone sa loob at sa labas ng kompanya?	4	2	0	0
	22	Pinipilit mo ba ang mga kasosyo sa negosyo na panatilihin ang kumpidensyalidad, tulad ng paglalagay ng mga pahayag ukol sa kumpidensyalidad (obligasyong panatilihin ang kumpidensyalidad) sa mga kontrata?	4	2	0	0
	23	Kinukumpirma mo ba ang kaligtasan ng serbisyo at relayabilidad sa pamamagitan ng pagsusuri sa mga termino ng paggamit at mga hakbang panseguridad bago pumili ng panlabas na serbisyo, tulad ng serbisyo na may kinalaman sa cloud?	4	2	0	0
	24	Nagsasagawa ba ng mga preparasyon kung may mangyaring insidente na may kinalaman sa seguridad ng impormasyon, tulad ng pagsasaayos ng mga pamamaraan sa pagtugon sa paglabas, pagkawala, o pagkanakaw ng kumpidensyal na impormasyon?	4	2	0	0
	25	Ibinigay mo ba ang depinisyon ng nilalaman ng mga hakbang sa seguridad ng impormasyon, tulad ng pagsasakatuparan ng mga ito (tulad ng sa 1 hanggang 24 sa itaas) bilang mga polisiya ng kompanya?	4	2	0	0

*1 Isang programang inilaan ng Microsoft Corporation upang ayusin ang mga depekto sa mga Window PC

*2 Isang database file na tinatawag na “pattern file” para sa pag-alam ng mga virus sa computer

*3 Ang pangkalahatang pangalan ng mga serbisyo na ginagamit sa pamamagitan ng Internet, tulad ng pagbabangko gamit ang Internet, social media, webmail, at mga kalendaryo

★ Walang garantiya na ang mga hakbang na isinalarawan sa talaan ng Pansariling Ebaluwasyon ng Kompanya ay naglalaan ng kumpletong proteksyon.

A Kabuuang bilang ng puntos sa pagpapatupad	B Kabuuang bilang ng puntos sa bahagyang pagpapatupad	A+B Puntos
Puntos	Puntos	Puntos

Unang Bahagi

Pangunahing mga hakbang

Ang mga bagay sa Bilang 1 hanggang 5 ay ang mga hakbang na kailangang maisagawa anuman ang laki o anyo ng kompanya. Napakahalaga na ang mga hakbang na ito ay patuloy na masuri at hindi lamang maisagawa nang isang beses. Kinakailangan na maipatupad ang mga ito bilang mga panuntunan sa kompanya nang sa gayon ay makasunod ang lahat ng mga empleyado dito.

Bilang 1 Mga hakbang sa bulnerabilidad

Palaging panatilihing bago ang iyong OS at software

Maaaring magdulot ng pinsala at magkaroon ng virus ang iyong device dahil sa pagsasawalang bahala sa mga isyu sa seguridad ng iyong OS at software. Tiyaking mag-update ng iyong OS at software sa pamamagitan ng mga patch o gumamit ng pinakabagong bersyon.

Aksyon **Magsagawa ng mga hakbang, tulad ng paggamit ng Windows Update (Windows OS) o gumamit ng pinakabagong bersyon ng Adobe Flash Player, Abobe Reader, Java runtime environment, at iba pang software.**

Bilang 2 Mga hakbang kontra sa virus

Mag-install ng antivirus software at gamitin ito nang naangkop.

Tumataas ang bilang ng mga virus na nagnanakaw ng mga ID at password, gumagamit ng mga computer kahit nasa ibang lugar, at biglaang nag-i-encrypt ng mga file. Tiyaking mag-install ng antivirus software at siguraduhing ang virus definition file (pattern file) ay palagiang bago.

Aksyon **Magsagawa ng mga hakbang, tulad ng pag-set ng iyong device na awtomatikong mag-update ng virus definition file at pag-isipang mag-install ng pinagsama-samang software para sa seguridad.**

Bilang 3 Pamamahala ng password

Gumamit ng hindi madaling matukoy na mga password

Tumataas ang bilang ng pinsala sa hindi awtorisadong mga pag-log in dahil madaling mahulaan ang mga password pati na rin ang kahina-hinalang paggamit ng mga ID at password na lumabas mula sa isang serbisyo sa web. Gawing mahirap ang iyong password sa pamamagitan ng pagpapahaba at pagpapakomplikado nito. Huwag itong gamiting muli.

*Simpleng password: Password na madaling mahulaan ng ikatlong partido, tulad ng iyong pangalan, pangalan ng kompanya, o simpleng mga salitang Ingles sa diksyunaryo.

Aksyon **Magsagawa ng mga hakbang, tulad ng paggamit ng mga password na kombinasyon ng 10 o higit pang mga karakter, numero, at simbolo. Huwag gumamit ng mga pangalan, numero ng telepono, petsa ng kaarawan, atbp., at huwag gumamit ng parehong password para sa iba't ibang mga serbisyo sa web at iba pang mga website.**

Bilang 4 Mga setting ng device

Suriin ang mga setting sa pagbabahagi

Mayroong tumataas na pag-aalala dahil nakikita ng mga hindi awtorisadong tao ang impormasyon bunsod sa mga datos na naimbak sa mga file server o online storage, o mga network copier na hindi na-configure nang tama. Tiyakin na ang mga server at ang mga network device ay naibahagi lamang sa mga tao na pinapayagang magkaroon ng akseso dito.

Aksyon **Magsagawa ng mga hakbang, tulad ng paglimita sa hangganan ng pagbabahagi ng mga serbisyo sa cloud, paglimita sa hangganan ng pagbabahagi ng mga device na konektado sa network, at pagbabago ng mga setting kapag ang mga empleyado ay nalipat sa ibang mga departamento o nagretiro.**

Bilang 5 Pagkalap ng mga impormasyon

Matuto tungkol sa panganib at mga paraan ng pag-atake at magsagawa ng mga hakbang upang malabanan ang mga ito.

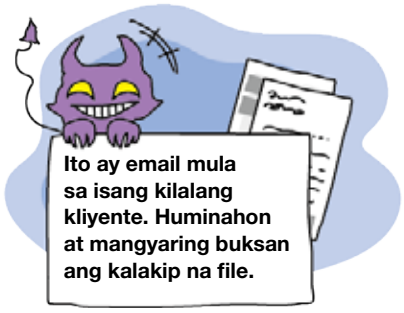
Tumataas ang bilang ng pagkalap at pagnanakaw ng mga ID at password sa pamamagitan ng email gamit ang mga virus na ginagaya ang mga kasosyo sa negosyo o iba pang mga stakeholder, o pinapasunod ang mga tao na mapunta sa kahina-hinalang mga web site na nanggagaya sa mga lehitimong mga web site. Magsagawa ng mga hakbang upang malabanan ang panganib at mga pamamaraan ng pag-atake sa pamamagitan ng pag-aaral tungkol sa mga ito.

Aksyon **Magsagawa ng mga hakbang, tulad ng pagsuri sa IPA website at pag-subscribe sa email magazine upang matuto tungkol sa bagong mga panganib at pamamaraan ng pag-atake, at pagkumpirma ng mga alerto na natanggap dahil sa pagbabangko gamit ang Internet at iba pang mga serbisyong ginagamit.**

Ikalawang Bahagi

Mga hakbang bilang isang empleyado

Ang tinutukoy ng Bilang 6 hanggang 18 ay mga bagay na dapat nababatid ng mga empleyado. Madaling magkamali ang tao dahil sa pamilyaridad ng pangangasiwa ng impormasyon araw-araw at maaaring makaligtaan. Dagdag pa, dahil sa pabago-bago ang uri ng panganib sa bawat araw, kailangang palaging malawak ang iyong pang-unawa.



Bilang 6 Mga panuntunan sa e-mail

Huwag basta magtitiwala sa ano mang mga e-mail na natanggap mula sa hindi kakilala

Maaari itong humantong sa impeksyon ng virus dahil sa pagbubukas ng mga kalakip sa email o dahil sa pag-click ng mga URL link sa mensahe sa email. Maging maingat sa mga ito lalo na kung galing sa mga hindi kakilala.

Aksyon **Magsagawa ng mga hakbang, tulad ng hindi pagbukas ng mga kalakip o sa pag-click ng mga URL link sa kahina-hinalang mga email, at i-report ito sa departamento ng seguridad upang magbahagi ng impormasyon tungkol sa mga kahina-hinalang mga email sa iyong kompanya.**

Bilang 7 Mga panuntunan sa email

Iwasang magpadala ng email sa maling resipiyente.

Magkakaroon ng mga insidente ng paglabas ng impormasyon sa mga hindi kakilala dahil sa pagkakamali ng pagpapadala ng mga e-mail o fax sa maling tao. Tiyaking suriing mabuti kung sino ang pinagpapadalhan ng mga email o fax. Dagdag pa, ang paglabas ng impormasyon ay nangyayari kung nagkamali ka sa pagbigay ng e-mail address. Kapag nagpapadala ng email sa maraming tao, tiyaking suriin ang mga email address ng mga tatanggap.

Aksyon **Magsagawa ng mga hakbang, tulad ng pagsuri nang dalawang beses sa mga address bago magpadala ng mga email o fax, at bukod na piliin ang mga address sa CC at BCC sa mga email.**

Bilang 8 Mga panuntunan sa email

Protektahan ang mahahalagang impormasyon kapag nagpapadala ng email

Kapag nagpapadala ng importanteng impormasyon sa pamamagitan ng e-mail, huwag itong isulat sa mismong email. Sa halip, isulat ito sa isang file, protektahan ito ng password, at ilakip ang file sa email. Bigyan ng notipikasyon tungkol sa password ang tatanggap ng email sa pamamagitan ng pagtawag sa kanila o sa pamamagitan ng ibang paraan, sa halip na isulat ito sa mismong e-mail.

Aksyon **Magsagawa ng mga hakbang, tulad ng pagsusulat ng importanteng impormasyon sa isang file at protektahan ito ng password. Bigyan ng notipikasyon ang tatanggap tungkol sa password sa pamamagitan ng telepono o ibang paraan.**

Bilang 9 Mga panuntunan sa wireless LAN

Iwasan ang makinig sa usapan ng iba at hindi awtorisadong paggamit ng mga wireless LAN.

Maaaring mabasa ang mga datos o magamit sa kriminal na mga gawain ang mga wirelss LAN na walang sapat na mga setting sa seguridad sa pamamagitan ng tahasang pagkonekta dito. Tiyaking i-set ang seguridad ng mga wireless LAN upang maiwasan ang pakikinig ng iba at ang hindi awtorisadong paggamit.

Aksyon **Magsagawa ng mg hakbang, tulad ng paggamit ng mga encryption setting (halimbawa WPA2-PSK) at pass phrase na mahaba at mahirap hulaan.**

Bilang 10 Mga panuntunan sa paggamit ng Internet

Iwasan ang alalahanin sa paggamit ng Internet

Ang pagtingin sa kahina-hinalang mga website o mga website na may problema sa seguridad ay maaaring magresulta sa pagkakaroon ng virus ng iyong device. Bilang karagdagan, maaaring mapinsala ang mga kompanya dahil sa praktikal na mga biro na nailathala sa social media o sa mga talaan ng mensahe o aksidenteng paglathala ng kumpidensyal na impormasyon. Kailangang maiwasan ang pinsala sa pamamagitan ng pagkakaroon ng sistema at mga panuntunan na humahadlang sa paggamit ng Internet sa trabaho.

Aksyon **Magsagawa ng mga hakbang, tulad ng paggawa ng panuntunan sa pag-akseso sa paggamit ng Internet at social media, at gumamit ng mga web filter upang sistematikong limitahan ang paggamit ng Internet.**

Bilang 11 Mga panuntunan sa pag-back up

Imungkahi ang regular na pag-back up

Ang mga datos sa iyong PC o server ay maaaring mawala dahil sa hindi paggana, maling operasyon, o impeksyon ng virus. Mag-back up ng mga datos upang paghandaan ang hindi inaasahang mga sitwasyon.

Aksyon **Magsagawa ng mga hakbang, tulad ng regular na pag-back up ng mga importanteng impormasyon at pag-save ng mga back up sa seperadong lokasyon.**

Paliwanag

Bilang 12 | Mga panuntunan sa pag-imbak

Importanteng impormasyon/kailangang mapangasiwaan ang mga dokumento nang tama

Delikadong mag-iwan ng impormasyon o mga dokumento sa lamesa nang walang nagbabantay sapagkat maaaring makuha o mabasa ang mga ito ng iba. Kailangang mapangasiwaan nang tama ang mga impormasyon o dokumento upang hindi ito makita o mahawakan ng iba at siguraduhin na hindi naiiwan ang mga ito. Tukukyin ang lokasyon ng imbakan para sa impormasyon o mga dokumento, ilabas ang mga ito kapag kailangan lang sa trabaho, at siguruhing itabi ang mga itong muli pagkatapos.

Aksyon — **Magsagawa ng mga hakbang, tulad ng pagpapanatiling malinis ang lamesa, pag-imbak ng importanteng impormasyon o mga dokumento sa isang nakakandadong kabinet.**

Bilang 13 | Mga panuntunan sa paglilipat

Ilipat ang importanteng impormasyon nang ligtas

Kapag naglalabas ng importanteng impormasyon sa kompanya, maaari itong manakaw o maiwala nang hindi inaasahan. Magsagawa ng hakbang habang maaga kapag gumagamit ng laptop o smartphone, tulad ng pag-set ng password o pag-encrypt ng mga datos ng mga file, nang sa gayon ang impormasyon ay hindi madaling makikita kung sakaling ito ay manakaw o mawala.

Aksyon — **Magsagawa ng mga hakbang, tulad ng mandatoryong pagkuha ng permiso upang ilipat ang importanteng impormasyon, pagsiguro na mayroong mga password ang mga laptop, smartphone, at USB stick, at huwag iwanan ang mga bagahe nang walang nagbabantay.**

Bilang 14 | Pamamahala sa kaligtasan ng opisina

Huwag payagang gamitin ng kahit sino ang mga device nang walang permiso

Huwag iwanang walang nagbabantay ang mga computer habang nasa trabaho. Ang naiwang PC na maaaring magamit ng kahit sino, tulad ng PC na maaaring makapag-log in kahit walang password, ay maaaring magamit nang hindi wasto. Magsagawa ng mga hakbang upang protektahan ang mga PC sa hindi awtorisadong paggamit.

Aksyon — **Magsagawa ng mga hakbang, tulad ng pagsara ng iyong PC kapag umaalis ka sa iyong lamesa, pagpatay ng PC kapag umaalis ka sa opisina nang buong araw, at iwasang magamit ng iba ang iyong PC.**

Bilang 15 | Pamamahala sa kaligtasan ng opisina

Kausapin ang mga tao na hindi mo makilala

Mayroong panganib na manakaw ang impormasyon kung hindi mo lilimitahan ang akseso ng mga hindi awtorisadong tao na pumapasok sa opisina. Tiyakin na ang hindi awtorisadong mga tao ay hindi maaaring magkaroon ng akseso sa mga lugar kung saan ang mahalagang impormasyon o mga dokumento ay nakaimbak, lalo na ang mga server, archive, at safe.

Aksyon — **Magsagawa ng mga hakbang, tulad ng pakikipag-usap sa kahit sinong hindi mo makilala sa opisina o maglagay ng mesa para sa tanggapan ng bisita.**

Bilang 16 | Pamamahala sa kaligtasan ng opisina

Magsagawa ng mga hakbang upang maiwasan ang pagnanakaw ng mga kasangkapan at kagamitan

Habang ang mga device tulad ng mga laptop computer, tablet, at USB stick ay madaling gamitin at dalhin kahit saan, ito rin ang maaaring dahilan kung bakit madaling mawala o manakaw ang mga ito. Kapag ang mga device na ito ay hindi ginagamit, magsagawa ng mga hakbang na ilagay ang mga ito sa mga ligtas na lugar, tulad ng sa naikakandadong drawer.

Aksyon — **Magsagawa ng mga hakbang, tulad ng pagsara sa mga laptop, tablet, at kagamitan (mga CD, USB stick, external hard drive, atbp.) sa mga drawer sa lamesa kapag umaalis sa opisina nang buong araw.**

Bilang 17 | Pamamahala sa kaligtasan ng opisina

Maging mapang-unawa sa pagsara ng mga pintuan ng opisina.

Makatutulong na mas mapagbuti ang pagiging responsable ng huling taong magsasara ng pinto sa pamamagitan ng pagtatala kung anong oras siya umalis ng opisina. Pamahalaan ang mga susi at mga rekord.

Aksyon — **Magsagawa ng mga hakbang, tulad ng pamamahala ng mga susi at pagpapanatili ng rekord ng huling tao sa opisina na nagsara ng pinto (petsa, oras, at pangalan).**

Bilang 18 | Ligtas na pagtatapon ng impormasyon

Burahin ang mahalagang impormasyon nang sa gayon ay hindi na ito magamit muli

Ang simpleng pagtatapon sa basurahan ng mga dokumentong naglalaman ng mahalagang impormasyon ay maaaring magresulta sa seryosong pagkalat nito dahil mababasa ng iba ang mga dokumento. Dagdag pa rito, ang mga impormasyon sa mga elektronikong mga device at elektronikong media ay maaaring makuhang muli kahit nabura na. Kapag nagtatapon ng mahalagang impormasyon, itapon ang bawat medium nang tama, tulad ng paggamit ng shredder o software na pambura ng mga datos.

Aksyon — **Magsagawa ng mga hakbang upang itapon ang mga impormasyon, tulad ng paggamit ng software na pambura ng mga datos, pisikal na pagsira sa mga ito, o paghingi ng tulong sa isang espesyalista upang burahin ito.**

limbak ang mga dokumento na naglalaman ng mahalagang impormasyon sa nakakandadong mga drawer.

Iwasan ang pagnanakaw ng mga device.

Isara ang pintuan ng opisina.

Ikatlong Bahagi

Mga hakbang para sa organisasyon

Ang bilang 19 hanggang 25 ay mga hakbang na dapat isagawa pagkatapos mabuo ang polisiya para sa organisasyon. Pagyamanin ang kaalaman ng empleyado sa pamamagitan ng klarong pagdudokumento ng mga panuntunan sa seguridad ng impormasyon at pagbabahagi nito sa opisina.

Bilang 19	Pagpapaalam sa obligasyon ng mga empleyado na panatilihin ang kumpidensyalidad

Ipaintindi sa mga empleyado ang kanilang obligasyon na panatilihin ang kumpidensyalidad

Kahit na sabihin na kailangang mapanatili ng mga empleyado ang kumpidensyalidad na nakasaad sa mga panuntunan ng kompanya, mabuting ipaalam nang klaro sa mga empleyado nito ang pagsunod sa mga panuntunan.

Aksyon	**Magsagawa ng mga hakbang, tulad ng pagpapaalam sa mga empleyado tungkol sa kanilang obligasyon na mapanatili ang kumpidensyalidad kapag sila ay natanggap sa trabaho.**

Bilang 20	Pagsasanay sa empleyado

Magsagawa ng regular na pagsasanay sa empleyado

Pinangangasiwaan ng mga empleyado ang impormasyon sa araw-araw sa kurso ng kanilang trabaho, at ang pamilyaridad na ito ay nangangahulugang mayroong mga tendensiyang may makaligtaan at nakalilimutan nilang pangasiwaan ang impormasyon nang may seguridad. Epektibo ang mga regular na empleyado sa pagtaas ng kaalaman ng ibang empleyado.

Aksyon	**Magsagawa ng mga aksyon, tulad ng regular na pagpapaliwanag ng kahalagahan ng pamamahala ng impormasyon at pagsasagawa ng pagsasanay sa loob ng kompanya.**

Bilang 21	Paggamit ng personal na mga device

Magpasya kung papayagan ang paggamit ng personal na mga device para sa trabaho

Nagiging mahirap ang pagsigurado ng seguridad kung ang personal na mga device tulad ng mga PC at smartphone ay ginagamit sa trabaho, dahil hindi magiging madaling pangasiwaan kung paano ito ginagamit ng mga empleyado. Magpasya kung ang mga personal na device ay maaaring gamitin sa trabaho at magpatupad ng mga panuntunan sa paggamit.

Aksyon	**Magsagawa ng mga hakbang, tulad ng pagbuo ng sistema sa pagbibigay ng permiso sa paggamit ng personal na mga device tulad ng mga PC at smartphone para sa trabaho at tiyakin ang mga panuntunan para sa paggamit ng mga ito kung papayagan sa trabaho.**

Bilang 22	Pamamahala ng kasosyo sa negosyo

Hilingin sa mga kasosyo sa negosyo na panatilihin ang kumpidensyalidad

Iwasang asahan na pananatilihin ng mga kasosyo sa negosyo ang kumpidensyalidad base sa uri ng impormasyon. Kapag nagbibigay ng kumpidensyal na impormasyon sa mga kasosyo sa negosyo, kailangang klaruhin na ito ay kumpidensyal.

Aksyon	**Magsagawa ng mga hakbang, tulad ng pagsulat ng mga kontrata na klarong nagsasaad na ang mga nilalaman nito ay dapat kumpidensyal.**

Bilang 23	Paggamit ng mga serbisyong panlabas

Gumamit ng pinagkakatiwalaang mga serbisyong panlabas

Kung pumili ka ng mga serbisyong panlabas, tulad ng serbisyong may kinalaman sa cloud, na may priyoridad sa gastos, maaaring hindi mo magagamit ang mga ito dahil sa hindi mga paggana at iba pang problema. Suriing mabuti ang paggana, relayabilidad, detalye ng kompensasyon, at iba pang mahahalagang konsiderasyon kapag gumagamit ng mga serbisyong panlabas para sa mga application na may mahalagang gampanin sa pagpapatuloy ng negosyo.

Aksyon	**Magsagawa ng mga hakbang, tulad ng pagsuri sa mga termino ng serbisyo, mga detalye ng kompensasyon, mga hakbang sa seguridad, at iba pang mahahalagang bagay sa pagpili ng tagapagbigay-serbisyo.**

Paliwanag

Bilang 24	Paghahanda para sa mga insidente sa seguridad ng impormasyon

Maghanda para sa mga insidente ng seguridad ng impormasyon nang maaga

Kapag may nangyaring insidente, kadalasan ay walang oras na makapag-isip nang kalmado, at maaaring bumagal ang pagresponde sa insidente dahil sa epekto nito. Sumangguni sa mga insidente na naibalita sa media bilang reperensya sa pag-iisip kung sino ang gagawa ng alin at kailan, umaasa na ang kaparehong insidente ang nangyayari sa iyong kompanya.

Aksyon	**Magsagawa ng mga hakbang, tulad ng pagsasaayos ng mga manwal sa pagresponde sa lumabas, nawala, o nanakaw na mahalagang impormasyon.**

Bilang 25	Paghahanda sa mga panuntunan

Gumawa ng mga panuntunan para sa mga hakbang sa seguridad ng impormasyon

Kahit na ang mga tagapagpaganap ay nagpapatupad ng mga polisiya para sa mga hakbang sa seguridad ng impormasyon, maliban kung ang mga ito ay nakadokumento nang malinaw bilang mga panuntunan sa loob ng opisina, kailangan ng mga empleyado na humingi ng payo sa kanilang mga tagapamahala sa lahat ng oras. Upang kusang mapasunod ang mga empleyado sa mga panuntunan, kinakailangang maidokumento nang malinaw ang “mga panuntunan ng kompanya” nang sa gayon ay maaaring sumangguni ang mga empleyado rito kahit anong oras.

Aksyon	**Magsagawa ng mga hakbang, tulad ng pagpapatupad ng bilang 1 hanggang 24 sa talaan ng ebaluwasyon para sa mga panuntunan sa mga hakbang sa seguridad ng impormasyon at ibahagi ang mga ito sa kompanya at regular na suriin ang mga panuntunang ito upang mapaunlad kung mayroon mang kakulangang makita.**

NISC National center of Incident readiness and Strategy for Cybersecurity

DICT Department of Information and Communications Technology

IPA Information-technology Promotion Agency, Japan

2019.04