

IT SMĚRNICE SPOLEČNOSTI TECHNOVA

Úvod

Tato směrnice definuje závazná pravidla pro používání informačních technologií ve společnosti TechNova. Jejím cílem je zajistit bezpečnost, dostupnost a integritu firemních dat a systémů. Směrnice je závazná pro všechny zaměstnance, externí spolupracovníky i dodavatele, kteří mají přístup k IT prostředkům společnosti.

Základní principy

Každý uživatel je odpovědný za bezpečné používání IT prostředků. Přístup k systémům je poskytován pouze v rozsahu nezbytném pro výkon pracovní role. Veškeré aktivity mohou být monitorovány za účelem zajištění bezpečnosti.

Správa hesel

Hesla představují základní bezpečnostní prvek. Je přísně zakázáno hesla sdílet, sdělovat třetím osobám nebo zapisovat na nechráněná místa.

Hesla musí být pravidelně měněna a musí splňovat bezpečnostní požadavky. Doporučuje se používat unikátní hesla pro každý systém.

Používání vícefaktorového ověřování je povinné tam, kde je dostupné.

Ukládání a správa dat

Firemní data musí být ukládána výhradně na schválená úložiště, jako jsou OneDrive a SharePoint. Tato úložiště jsou pravidelně zálohována a splňují bezpečnostní standardy.

Je zakázáno ukládat firemní data na osobní zařízení, externí disky bez schválení nebo na neautorizované cloudové služby.

Sdílení dat mimo organizaci musí být vždy schváleno.

Používání zařízení

Firemní zařízení slouží primárně k pracovním účelům. Každé zařízení musí být zabezpečeno heslem nebo biometrickým prvkem.

Při opuštění pracovního místa je uživatel povinen zařízení uzamknout.

Instalace softwaru

Instalace softwaru podléhá schválení IT oddělení. Používání nelegálního nebo neověřeného softwaru je zakázáno.

Přístup k internetu

Je zakázáno nahrávat firemní data na cizí webové služby, které nejsou schváleny společností.

Používání veřejných WiFi sítí bez VPN je považováno za rizikové.

Bezpečnostní incidenty

Každý zaměstnanec je povinen neprodleně nahlásit jakýkoliv bezpečnostní incident. To zahrnuje podezřelé emaily, ztrátu zařízení nebo neoprávněný přístup.

Zálohování

Data uložená na schválených platformách jsou pravidelně zálohována. Uživatel nesmí obcházet tyto mechanismy.

Mobilní zařízení

Mobilní zařízení musí být zabezpečena a registrována v systému správy zařízení. V případě ztráty musí být okamžitě nahlášena.

Práce na dálku

Při práci mimo kancelář je nutné používat VPN a dodržovat stejné bezpečnostní standardy jako v kanceláři.

Kontrola a sankce

Porušení této směrnice může vést k disciplinárním opatřením včetně ukončení pracovního poměru.

Závěr

Dodržování této směrnice je klíčové pro ochranu společnosti TechNova. Každý zaměstnanec je povinen se s ní seznámit a řídit se jí.

IT SMĚRNICE SPOLEČNOSTI TECHNOVA

Úvod

Tato směrnice definuje závazná pravidla pro používání informačních technologií ve společnosti TechNova. Jejím cílem je zajistit bezpečnost, dostupnost a integritu firemních dat a systémů. Směrnice je závazná pro všechny zaměstnance, externí spolupracovníky i dodavatele, kteří mají přístup k IT prostředkům společnosti.

Základní principy

Každý uživatel je odpovědný za bezpečné používání IT prostředků. Přístup k systémům je poskytován pouze v rozsahu nezbytném pro výkon pracovní role. Veškeré aktivity mohou být monitorovány za účelem zajištění bezpečnosti.

Správa hesel

Hesla představují základní bezpečnostní prvek. Je přísně zakázáno hesla sdílet, sdělovat třetím osobám nebo zapisovat na nechráněná místa.

Hesla musí být pravidelně měněna a musí splňovat bezpečnostní požadavky. Doporučuje se používat unikátní hesla pro každý systém.

Používání vícefaktorového ověřování je povinné tam, kde je dostupné.

Ukládání a správa dat

Firemní data musí být ukládána výhradně na schválená úložiště, jako jsou OneDrive a SharePoint. Tato úložiště jsou pravidelně zálohována a splňují bezpečnostní standardy.

Je zakázáno ukládat firemní data na osobní zařízení, externí disky bez schválení nebo na neautorizované cloudové služby.

Sdílení dat mimo organizaci musí být vždy schváleno.

Používání zařízení

Firemní zařízení slouží primárně k pracovním účelům. Každé zařízení musí být zabezpečeno heslem nebo biometrickým prvkem.

Při opuštění pracovního místa je uživatel povinen zařízení uzamknout.

Instalace softwaru

Instalace softwaru podléhá schválení IT oddělení. Používání nelegálního nebo neověřeného softwaru je zakázáno.

Přístup k internetu

Je zakázáno nahrávat firemní data na cizí webové služby, které nejsou schváleny společností.

Používání veřejných WiFi sítí bez VPN je považováno za rizikové.

Bezpečnostní incidenty

Každý zaměstnanec je povinen neprodleně nahlásit jakýkoliv bezpečnostní incident. To zahrnuje podezřelé emaily, ztrátu zařízení nebo neoprávněný přístup.

Zálohování

Data uložená na schválených platformách jsou pravidelně zálohována. Uživatel nesmí obcházet tyto mechanismy.

Mobilní zařízení

Mobilní zařízení musí být zabezpečena a registrována v systému správy zařízení. V případě ztráty musí být okamžitě nahlášena.

Práce na dálku

Při práci mimo kancelář je nutné používat VPN a dodržovat stejné bezpečnostní standardy jako v kanceláři.

Kontrola a sankce

Porušení této směrnice může vést k disciplinárním opatřením včetně ukončení pracovního poměru.

Závěr

Dodržování této směrnice je klíčové pro ochranu společnosti TechNova. Každý zaměstnanec je povinen se s ní seznámit a řídit se jí.

IT SMĚRNICE SPOLEČNOSTI TECHNOVA

Úvod

Tato směrnice definuje závazná pravidla pro používání informačních technologií ve společnosti TechNova. Jejím cílem je zajistit bezpečnost, dostupnost a integritu firemních dat a systémů. Směrnice je závazná pro všechny zaměstnance, externí spolupracovníky i dodavatele, kteří mají přístup k IT prostředkům společnosti.

Základní principy

Každý uživatel je odpovědný za bezpečné používání IT prostředků. Přístup k systémům je poskytován pouze v rozsahu nezbytném pro výkon pracovní role. Veškeré aktivity mohou být monitorovány za účelem zajištění bezpečnosti.

Správa hesel

Hesla představují základní bezpečnostní prvek. Je přísně zakázáno hesla sdílet, sdělovat třetím osobám nebo zapisovat na nechráněná místa.

Hesla musí být pravidelně měněna a musí splňovat bezpečnostní požadavky. Doporučuje se používat unikátní hesla pro každý systém.

Používání vícefaktorového ověřování je povinné tam, kde je dostupné.

Ukládání a správa dat

Firemní data musí být ukládána výhradně na schválená úložiště, jako jsou OneDrive a SharePoint. Tato úložiště jsou pravidelně zálohována a splňují bezpečnostní standardy.

Je zakázáno ukládat firemní data na osobní zařízení, externí disky bez schválení nebo na neautorizované cloudové služby.

Sdílení dat mimo organizaci musí být vždy schváleno.

Používání zařízení

Firemní zařízení slouží primárně k pracovním účelům. Každé zařízení musí být zabezpečeno heslem nebo biometrickým prvkem.

Při opuštění pracovního místa je uživatel povinen zařízení uzamknout.

Instalace softwaru

Instalace softwaru podléhá schválení IT oddělení. Používání nelegálního nebo neověřeného softwaru je zakázáno.

Přístup k internetu

Je zakázáno nahrávat firemní data na cizí webové služby, které nejsou schváleny společností.

Používání veřejných WiFi sítí bez VPN je považováno za rizikové.

Bezpečnostní incidenty

Každý zaměstnanec je povinen neprodleně nahlásit jakýkoliv bezpečnostní incident. To zahrnuje podezřelé emaily, ztrátu zařízení nebo neoprávněný přístup.

Zálohování

Data uložená na schválených platformách jsou pravidelně zálohována. Uživatel nesmí obcházet tyto mechanismy.

Mobilní zařízení

Mobilní zařízení musí být zabezpečena a registrována v systému správy zařízení. V případě ztráty musí být okamžitě nahlášena.

Práce na dálku

Při práci mimo kancelář je nutné používat VPN a dodržovat stejné bezpečnostní standardy jako v kanceláři.

Kontrola a sankce

Porušení této směrnice může vést k disciplinárním opatřením včetně ukončení pracovního poměru.

Závěr

Dodržování této směrnice je klíčové pro ochranu společnosti TechNova. Každý zaměstnanec je povinen se s ní seznámit a řídit se jí.

IT SMĚRNICE SPOLEČNOSTI TECHNOVA

Úvod

Tato směrnice definuje závazná pravidla pro používání informačních technologií ve společnosti TechNova. Jejím cílem je zajistit bezpečnost, dostupnost a integritu firemních dat a systémů. Směrnice je závazná pro všechny zaměstnance, externí spolupracovníky i dodavatele, kteří mají přístup k IT prostředkům společnosti.

Základní principy

Každý uživatel je odpovědný za bezpečné používání IT prostředků. Přístup k systémům je poskytován pouze v rozsahu nezbytném pro výkon pracovní role. Veškeré aktivity mohou být monitorovány za účelem zajištění bezpečnosti.

Správa hesel

Hesla představují základní bezpečnostní prvek. Je přísně zakázáno hesla sdílet, sdělovat třetím osobám nebo zapisovat na nechráněná místa.

Hesla musí být pravidelně měněna a musí splňovat bezpečnostní požadavky. Doporučuje se používat unikátní hesla pro každý systém.

Používání vícefaktorového ověřování je povinné tam, kde je dostupné.

Ukládání a správa dat

Firemní data musí být ukládána výhradně na schválená úložiště, jako jsou OneDrive a SharePoint. Tato úložiště jsou pravidelně zálohována a splňují bezpečnostní standardy.

Je zakázáno ukládat firemní data na osobní zařízení, externí disky bez schválení nebo na neautorizované cloudové služby.

Sdílení dat mimo organizaci musí být vždy schváleno.

Používání zařízení

Firemní zařízení slouží primárně k pracovním účelům. Každé zařízení musí být zabezpečeno heslem nebo biometrickým prvkem.

Při opuštění pracovního místa je uživatel povinen zařízení uzamknout.

Instalace softwaru

Instalace softwaru podléhá schválení IT oddělení. Používání nelegálního nebo neověřeného softwaru je zakázáno.

Přístup k internetu

Je zakázáno nahrávat firemní data na cizí webové služby, které nejsou schváleny společností.

Používání veřejných WiFi sítí bez VPN je považováno za rizikové.

Bezpečnostní incidenty

Každý zaměstnanec je povinen neprodleně nahlásit jakýkoliv bezpečnostní incident. To zahrnuje podezřelé emaily, ztrátu zařízení nebo neoprávněný přístup.

Zálohování

Data uložená na schválených platformách jsou pravidelně zálohována. Uživatel nesmí obcházet tyto mechanismy.

Mobilní zařízení

Mobilní zařízení musí být zabezpečena a registrována v systému správy zařízení. V případě ztráty musí být okamžitě nahlášena.

Práce na dálku

Při práci mimo kancelář je nutné používat VPN a dodržovat stejné bezpečnostní standardy jako v kanceláři.

Kontrola a sankce

Porušení této směrnice může vést k disciplinárním opatřením včetně ukončení pracovního poměru.

Závěr

Dodržování této směrnice je klíčové pro ochranu společnosti TechNova. Každý zaměstnanec je povinen se s ní seznámit a řídit se jí.

IT SMĚRNICE SPOLEČNOSTI TECHNOVA

Úvod

Tato směrnice definuje závazná pravidla pro používání informačních technologií ve společnosti TechNova. Jejím cílem je zajistit bezpečnost, dostupnost a integritu firemních dat a systémů. Směrnice je závazná pro všechny zaměstnance, externí spolupracovníky i dodavatele, kteří mají přístup k IT prostředkům společnosti.

Základní principy

Každý uživatel je odpovědný za bezpečné používání IT prostředků. Přístup k systémům je poskytován pouze v rozsahu nezbytném pro výkon pracovní role. Veškeré aktivity mohou být monitorovány za účelem zajištění bezpečnosti.

Správa hesel

Hesla představují základní bezpečnostní prvek. Je přísně zakázáno hesla sdílet, sdělovat třetím osobám nebo zapisovat na nechráněná místa.

Hesla musí být pravidelně měněna a musí splňovat bezpečnostní požadavky. Doporučuje se používat unikátní hesla pro každý systém.

Používání vícefaktorového ověřování je povinné tam, kde je dostupné.

Ukládání a správa dat

Firemní data musí být ukládána výhradně na schválená úložiště, jako jsou OneDrive a SharePoint. Tato úložiště jsou pravidelně zálohována a splňují bezpečnostní standardy.

Je zakázáno ukládat firemní data na osobní zařízení, externí disky bez schválení nebo na neautorizované cloudové služby.

Sdílení dat mimo organizaci musí být vždy schváleno.

Používání zařízení

Firemní zařízení slouží primárně k pracovním účelům. Každé zařízení musí být zabezpečeno heslem nebo biometrickým prvkem.

Při opuštění pracovního místa je uživatel povinen zařízení uzamknout.

Instalace softwaru

Instalace softwaru podléhá schválení IT oddělení. Používání nelegálního nebo neověřeného softwaru je zakázáno.

Přístup k internetu

Je zakázáno nahrávat firemní data na cizí webové služby, které nejsou schváleny společností.

Používání veřejných WiFi sítí bez VPN je považováno za rizikové.

Bezpečnostní incidenty

Každý zaměstnanec je povinen neprodleně nahlásit jakýkoliv bezpečnostní incident. To zahrnuje podezřelé emaily, ztrátu zařízení nebo neoprávněný přístup.

Zálohování

Data uložená na schválených platformách jsou pravidelně zálohována. Uživatel nesmí obcházet tyto mechanismy.

Mobilní zařízení

Mobilní zařízení musí být zabezpečena a registrována v systému správy zařízení. V případě ztráty musí být okamžitě nahlášena.

Práce na dálku

Při práci mimo kancelář je nutné používat VPN a dodržovat stejné bezpečnostní standardy jako v kanceláři.

Kontrola a sankce

Porušení této směrnice může vést k disciplinárním opatřením včetně ukončení pracovního poměru.

Závěr

Dodržování této směrnice je klíčové pro ochranu společnosti TechNova. Každý zaměstnanec je povinen se s ní seznámit a řídit se jí.

IT SMĚRNICE SPOLEČNOSTI TECHNOVA

Úvod

Tato směrnice definuje závazná pravidla pro používání informačních technologií ve společnosti TechNova. Jejím cílem je zajistit bezpečnost, dostupnost a integritu firemních dat a systémů. Směrnice je závazná pro všechny zaměstnance, externí spolupracovníky i dodavatele, kteří mají přístup k IT prostředkům společnosti.

Základní principy

Každý uživatel je odpovědný za bezpečné používání IT prostředků. Přístup k systémům je poskytován pouze v rozsahu nezbytném pro výkon pracovní role. Veškeré aktivity mohou být monitorovány za účelem zajištění bezpečnosti.

Správa hesel

Hesla představují základní bezpečnostní prvek. Je přísně zakázáno hesla sdílet, sdělovat třetím osobám nebo zapisovat na nechráněná místa.

Hesla musí být pravidelně měněna a musí splňovat bezpečnostní požadavky. Doporučuje se používat unikátní hesla pro každý systém.

Používání vícefaktorového ověřování je povinné tam, kde je dostupné.

Ukládání a správa dat

Firemní data musí být ukládána výhradně na schválená úložiště, jako jsou OneDrive a SharePoint. Tato úložiště jsou pravidelně zálohována a splňují bezpečnostní standardy.

Je zakázáno ukládat firemní data na osobní zařízení, externí disky bez schválení nebo na neautorizované cloudové služby.

Sdílení dat mimo organizaci musí být vždy schváleno.

Používání zařízení

Firemní zařízení slouží primárně k pracovním účelům. Každé zařízení musí být zabezpečeno heslem nebo biometrickým prvkem.

Při opuštění pracovního místa je uživatel povinen zařízení uzamknout.

Instalace softwaru

Instalace softwaru podléhá schválení IT oddělení. Používání nelegálního nebo neověřeného softwaru je zakázáno.

Přístup k internetu

Je zakázáno nahrávat firemní data na cizí webové služby, které nejsou schváleny společností.

Používání veřejných WiFi sítí bez VPN je považováno za rizikové.

Bezpečnostní incidenty

Každý zaměstnanec je povinen neprodleně nahlásit jakýkoliv bezpečnostní incident. To zahrnuje podezřelé emaily, ztrátu zařízení nebo neoprávněný přístup.

Zálohování

Data uložená na schválených platformách jsou pravidelně zálohována. Uživatel nesmí obcházet tyto mechanismy.

Mobilní zařízení

Mobilní zařízení musí být zabezpečena a registrována v systému správy zařízení. V případě ztráty musí být okamžitě nahlášena.

Práce na dálku

Při práci mimo kancelář je nutné používat VPN a dodržovat stejné bezpečnostní standardy jako v kanceláři.

Kontrola a sankce

Porušení této směrnice může vést k disciplinárním opatřením včetně ukončení pracovního poměru.

Závěr

Dodržování této směrnice je klíčové pro ochranu společnosti TechNova. Každý zaměstnanec je povinen se s ní seznámit a řídit se jí.

IT SMĚRNICE SPOLEČNOSTI TECHNOVA

Úvod

Tato směrnice definuje závazná pravidla pro používání informačních technologií ve společnosti TechNova. Jejím cílem je zajistit bezpečnost, dostupnost a integritu firemních dat a systémů. Směrnice je závazná pro všechny zaměstnance, externí spolupracovníky i dodavatele, kteří mají přístup k IT prostředkům společnosti.

Základní principy

Každý uživatel je odpovědný za bezpečné používání IT prostředků. Přístup k systémům je poskytován pouze v rozsahu nezbytném pro výkon pracovní role. Veškeré aktivity mohou být monitorovány za účelem zajištění bezpečnosti.

Správa hesel

Hesla představují základní bezpečnostní prvek. Je přísně zakázáno hesla sdílet, sdělovat třetím osobám nebo zapisovat na nechráněná místa.

Hesla musí být pravidelně měněna a musí splňovat bezpečnostní požadavky. Doporučuje se používat unikátní hesla pro každý systém.

Používání vícefaktorového ověřování je povinné tam, kde je dostupné.

Ukládání a správa dat

Firemní data musí být ukládána výhradně na schválená úložiště, jako jsou OneDrive a SharePoint. Tato úložiště jsou pravidelně zálohována a splňují bezpečnostní standardy.

Je zakázáno ukládat firemní data na osobní zařízení, externí disky bez schválení nebo na neautorizované cloudové služby.

Sdílení dat mimo organizaci musí být vždy schváleno.

Používání zařízení

Firemní zařízení slouží primárně k pracovním účelům. Každé zařízení musí být zabezpečeno heslem nebo biometrickým prvkem.

Při opuštění pracovního místa je uživatel povinen zařízení uzamknout.

Instalace softwaru

Instalace softwaru podléhá schválení IT oddělení. Používání nelegálního nebo neověřeného softwaru je zakázáno.

Přístup k internetu

Je zakázáno nahrávat firemní data na cizí webové služby, které nejsou schváleny společností.

Používání veřejných WiFi sítí bez VPN je považováno za rizikové.

Bezpečnostní incidenty

Každý zaměstnanec je povinen neprodleně nahlásit jakýkoliv bezpečnostní incident. To zahrnuje podezřelé emaily, ztrátu zařízení nebo neoprávněný přístup.

Zálohování

Data uložená na schválených platformách jsou pravidelně zálohována. Uživatel nesmí obcházet tyto mechanismy.

Mobilní zařízení

Mobilní zařízení musí být zabezpečena a registrována v systému správy zařízení. V případě ztráty musí být okamžitě nahlášena.

Práce na dálku

Při práci mimo kancelář je nutné používat VPN a dodržovat stejné bezpečnostní standardy jako v kanceláři.

Kontrola a sankce

Porušení této směrnice může vést k disciplinárním opatřením včetně ukončení pracovního poměru.

Závěr

Dodržování této směrnice je klíčové pro ochranu společnosti TechNova. Každý zaměstnanec je povinen se s ní seznámit a řídit se jí.

IT SMĚRNICE SPOLEČNOSTI TECHNOVA

Úvod

Tato směrnice definuje závazná pravidla pro používání informačních technologií ve společnosti TechNova. Jejím cílem je zajistit bezpečnost, dostupnost a integritu firemních dat a systémů. Směrnice je závazná pro všechny zaměstnance, externí spolupracovníky i dodavatele, kteří mají přístup k IT prostředkům společnosti.

Základní principy

Každý uživatel je odpovědný za bezpečné používání IT prostředků. Přístup k systémům je poskytován pouze v rozsahu nezbytném pro výkon pracovní role. Veškeré aktivity mohou být monitorovány za účelem zajištění bezpečnosti.

Správa hesel

Hesla představují základní bezpečnostní prvek. Je přísně zakázáno hesla sdílet, sdělovat třetím osobám nebo zapisovat na nechráněná místa.

Hesla musí být pravidelně měněna a musí splňovat bezpečnostní požadavky. Doporučuje se používat unikátní hesla pro každý systém.

Používání vícefaktorového ověřování je povinné tam, kde je dostupné.

Ukládání a správa dat

Firemní data musí být ukládána výhradně na schválená úložiště, jako jsou OneDrive a SharePoint. Tato úložiště jsou pravidelně zálohována a splňují bezpečnostní standardy.

Je zakázáno ukládat firemní data na osobní zařízení, externí disky bez schválení nebo na neautorizované cloudové služby.

Sdílení dat mimo organizaci musí být vždy schváleno.

Používání zařízení

Firemní zařízení slouží primárně k pracovním účelům. Každé zařízení musí být zabezpečeno heslem nebo biometrickým prvkem.

Při opuštění pracovního místa je uživatel povinen zařízení uzamknout.

Instalace softwaru

Instalace softwaru podléhá schválení IT oddělení. Používání nelegálního nebo neověřeného softwaru je zakázáno.

Přístup k internetu

Je zakázáno nahrávat firemní data na cizí webové služby, které nejsou schváleny společností.

Používání veřejných WiFi sítí bez VPN je považováno za rizikové.

Bezpečnostní incidenty

Každý zaměstnanec je povinen neprodleně nahlásit jakýkoliv bezpečnostní incident. To zahrnuje podezřelé emaily, ztrátu zařízení nebo neoprávněný přístup.

Zálohování

Data uložená na schválených platformách jsou pravidelně zálohována. Uživatel nesmí obcházet tyto mechanismy.

Mobilní zařízení

Mobilní zařízení musí být zabezpečena a registrována v systému správy zařízení. V případě ztráty musí být okamžitě nahlášena.

Práce na dálku

Při práci mimo kancelář je nutné používat VPN a dodržovat stejné bezpečnostní standardy jako v kanceláři.

Kontrola a sankce

Porušení této směrnice může vést k disciplinárním opatřením včetně ukončení pracovního poměru.

Závěr

Dodržování této směrnice je klíčové pro ochranu společnosti TechNova. Každý zaměstnanec je povinen se s ní seznámit a řídit se jí.

IT SMĚRNICE SPOLEČNOSTI TECHNOVA

Úvod

Tato směrnice definuje závazná pravidla pro používání informačních technologií ve společnosti TechNova. Jejím cílem je zajistit bezpečnost, dostupnost a integritu firemních dat a systémů. Směrnice je závazná pro všechny zaměstnance, externí spolupracovníky i dodavatele, kteří mají přístup k IT prostředkům společnosti.

Základní principy

Každý uživatel je odpovědný za bezpečné používání IT prostředků. Přístup k systémům je poskytován pouze v rozsahu nezbytném pro výkon pracovní role. Veškeré aktivity mohou být monitorovány za účelem zajištění bezpečnosti.

Správa hesel

Hesla představují základní bezpečnostní prvek. Je přísně zakázáno hesla sdílet, sdělovat třetím osobám nebo zapisovat na nechráněná místa.

Hesla musí být pravidelně měněna a musí splňovat bezpečnostní požadavky. Doporučuje se používat unikátní hesla pro každý systém.

Používání vícefaktorového ověřování je povinné tam, kde je dostupné.

Ukládání a správa dat

Firemní data musí být ukládána výhradně na schválená úložiště, jako jsou OneDrive a SharePoint. Tato úložiště jsou pravidelně zálohována a splňují bezpečnostní standardy.

Je zakázáno ukládat firemní data na osobní zařízení, externí disky bez schválení nebo na neautorizované cloudové služby.

Sdílení dat mimo organizaci musí být vždy schváleno.

Používání zařízení

Firemní zařízení slouží primárně k pracovním účelům. Každé zařízení musí být zabezpečeno heslem nebo biometrickým prvkem.

Při opuštění pracovního místa je uživatel povinen zařízení uzamknout.

Instalace softwaru

Instalace softwaru podléhá schválení IT oddělení. Používání nelegálního nebo neověřeného softwaru je zakázáno.

Přístup k internetu

Je zakázáno nahrávat firemní data na cizí webové služby, které nejsou schváleny společností.

Používání veřejných WiFi sítí bez VPN je považováno za rizikové.

Bezpečnostní incidenty

Každý zaměstnanec je povinen neprodleně nahlásit jakýkoliv bezpečnostní incident. To zahrnuje podezřelé emaily, ztrátu zařízení nebo neoprávněný přístup.

Zálohování

Data uložená na schválených platformách jsou pravidelně zálohována. Uživatel nesmí obcházet tyto mechanismy.

Mobilní zařízení

Mobilní zařízení musí být zabezpečena a registrována v systému správy zařízení. V případě ztráty musí být okamžitě nahlášena.

Práce na dálku

Při práci mimo kancelář je nutné používat VPN a dodržovat stejné bezpečnostní standardy jako v kanceláři.

Kontrola a sankce

Porušení této směrnice může vést k disciplinárním opatřením včetně ukončení pracovního poměru.

Závěr

Dodržování této směrnice je klíčové pro ochranu společnosti TechNova. Každý zaměstnanec je povinen se s ní seznámit a řídit se jí.

IT SMĚRNICE SPOLEČNOSTI TECHNOVA

Úvod

Tato směrnice definuje závazná pravidla pro používání informačních technologií ve společnosti TechNova. Jejím cílem je zajistit bezpečnost, dostupnost a integritu firemních dat a systémů. Směrnice je závazná pro všechny zaměstnance, externí spolupracovníky i dodavatele, kteří mají přístup k IT prostředkům společnosti.

Základní principy

Každý uživatel je odpovědný za bezpečné používání IT prostředků. Přístup k systémům je poskytován pouze v rozsahu nezbytném pro výkon pracovní role. Veškeré aktivity mohou být monitorovány za účelem zajištění bezpečnosti.

Správa hesel

Hesla představují základní bezpečnostní prvek. Je přísně zakázáno hesla sdílet, sdělovat třetím osobám nebo zapisovat na nechráněná místa.

Hesla musí být pravidelně měněna a musí splňovat bezpečnostní požadavky. Doporučuje se používat unikátní hesla pro každý systém.

Používání vícefaktorového ověřování je povinné tam, kde je dostupné.

Ukládání a správa dat

Firemní data musí být ukládána výhradně na schválená úložiště, jako jsou OneDrive a SharePoint. Tato úložiště jsou pravidelně zálohována a splňují bezpečnostní standardy.

Je zakázáno ukládat firemní data na osobní zařízení, externí disky bez schválení nebo na neautorizované cloudové služby.

Sdílení dat mimo organizaci musí být vždy schváleno.

Používání zařízení

Firemní zařízení slouží primárně k pracovním účelům. Každé zařízení musí být zabezpečeno heslem nebo biometrickým prvkem.

Při opuštění pracovního místa je uživatel povinen zařízení uzamknout.

Instalace softwaru

Instalace softwaru podléhá schválení IT oddělení. Používání nelegálního nebo neověřeného softwaru je zakázáno.

Přístup k internetu

Je zakázáno nahrávat firemní data na cizí webové služby, které nejsou schváleny společností.

Používání veřejných WiFi sítí bez VPN je považováno za rizikové.

Bezpečnostní incidenty

Každý zaměstnanec je povinen neprodleně nahlásit jakýkoliv bezpečnostní incident. To zahrnuje podezřelé emaily, ztrátu zařízení nebo neoprávněný přístup.

Zálohování

Data uložená na schválených platformách jsou pravidelně zálohována. Uživatel nesmí obcházet tyto mechanismy.

Mobilní zařízení

Mobilní zařízení musí být zabezpečena a registrována v systému správy zařízení. V případě ztráty musí být okamžitě nahlášena.

Práce na dálku

Při práci mimo kancelář je nutné používat VPN a dodržovat stejné bezpečnostní standardy jako v kanceláři.

Kontrola a sankce

Porušení této směrnice může vést k disciplinárním opatřením včetně ukončení pracovního poměru.

Závěr

Dodržování této směrnice je klíčové pro ochranu společnosti TechNova. Každý zaměstnanec je povinen se s ní seznámit a řídit se jí.

IT SMĚRNICE SPOLEČNOSTI TECHNOVA

Úvod

Tato směrnice definuje závazná pravidla pro používání informačních technologií ve společnosti TechNova. Jejím cílem je zajistit bezpečnost, dostupnost a integritu firemních dat a systémů. Směrnice je závazná pro všechny zaměstnance, externí spolupracovníky i dodavatele, kteří mají přístup k IT prostředkům společnosti.

Základní principy

Každý uživatel je odpovědný za bezpečné používání IT prostředků. Přístup k systémům je poskytován pouze v rozsahu nezbytném pro výkon pracovní role. Veškeré aktivity mohou být monitorovány za účelem zajištění bezpečnosti.

Správa hesel

Hesla představují základní bezpečnostní prvek. Je přísně zakázáno hesla sdílet, sdělovat třetím osobám nebo zapisovat na nechráněná místa.

Hesla musí být pravidelně měněna a musí splňovat bezpečnostní požadavky. Doporučuje se používat unikátní hesla pro každý systém.

Používání vícefaktorového ověřování je povinné tam, kde je dostupné.

Ukládání a správa dat

Firemní data musí být ukládána výhradně na schválená úložiště, jako jsou OneDrive a SharePoint. Tato úložiště jsou pravidelně zálohována a splňují bezpečnostní standardy.

Je zakázáno ukládat firemní data na osobní zařízení, externí disky bez schválení nebo na neautorizované cloudové služby.

Sdílení dat mimo organizaci musí být vždy schváleno.

Používání zařízení

Firemní zařízení slouží primárně k pracovním účelům. Každé zařízení musí být zabezpečeno heslem nebo biometrickým prvkem.

Při opuštění pracovního místa je uživatel povinen zařízení uzamknout.

Instalace softwaru

Instalace softwaru podléhá schválení IT oddělení. Používání nelegálního nebo neověřeného softwaru je zakázáno.

Přístup k internetu

Je zakázáno nahrávat firemní data na cizí webové služby, které nejsou schváleny společností.

Používání veřejných WiFi sítí bez VPN je považováno za rizikové.

Bezpečnostní incidenty

Každý zaměstnanec je povinen neprodleně nahlásit jakýkoliv bezpečnostní incident. To zahrnuje podezřelé emaily, ztrátu zařízení nebo neoprávněný přístup.

Zálohování

Data uložená na schválených platformách jsou pravidelně zálohována. Uživatel nesmí obcházet tyto mechanismy.

Mobilní zařízení

Mobilní zařízení musí být zabezpečena a registrována v systému správy zařízení. V případě ztráty musí být okamžitě nahlášena.

Práce na dálku

Při práci mimo kancelář je nutné používat VPN a dodržovat stejné bezpečnostní standardy jako v kanceláři.

Kontrola a sankce

Porušení této směrnice může vést k disciplinárním opatřením včetně ukončení pracovního poměru.

Závěr

Dodržování této směrnice je klíčové pro ochranu společnosti TechNova. Každý zaměstnanec je povinen se s ní seznámit a řídit se jí.

IT SMĚRNICE SPOLEČNOSTI TECHNOVA

Úvod

Tato směrnice definuje závazná pravidla pro používání informačních technologií ve společnosti TechNova. Jejím cílem je zajistit bezpečnost, dostupnost a integritu firemních dat a systémů. Směrnice je závazná pro všechny zaměstnance, externí spolupracovníky i dodavatele, kteří mají přístup k IT prostředkům společnosti.

Základní principy

Každý uživatel je odpovědný za bezpečné používání IT prostředků. Přístup k systémům je poskytován pouze v rozsahu nezbytném pro výkon pracovní role. Veškeré aktivity mohou být monitorovány za účelem zajištění bezpečnosti.

Správa hesel

Hesla představují základní bezpečnostní prvek. Je přísně zakázáno hesla sdílet, sdělovat třetím osobám nebo zapisovat na nechráněná místa.

Hesla musí být pravidelně měněna a musí splňovat bezpečnostní požadavky. Doporučuje se používat unikátní hesla pro každý systém.

Používání vícefaktorového ověřování je povinné tam, kde je dostupné.

Ukládání a správa dat

Firemní data musí být ukládána výhradně na schválená úložiště, jako jsou OneDrive a SharePoint. Tato úložiště jsou pravidelně zálohována a splňují bezpečnostní standardy.

Je zakázáno ukládat firemní data na osobní zařízení, externí disky bez schválení nebo na neautorizované cloudové služby.

Sdílení dat mimo organizaci musí být vždy schváleno.

Používání zařízení

Firemní zařízení slouží primárně k pracovním účelům. Každé zařízení musí být zabezpečeno heslem nebo biometrickým prvkem.

Při opuštění pracovního místa je uživatel povinen zařízení uzamknout.

Instalace softwaru

Instalace softwaru podléhá schválení IT oddělení. Používání nelegálního nebo neověřeného softwaru je zakázáno.

Přístup k internetu

Je zakázáno nahrávat firemní data na cizí webové služby, které nejsou schváleny společností.

Používání veřejných WiFi sítí bez VPN je považováno za rizikové.

Bezpečnostní incidenty

Každý zaměstnanec je povinen neprodleně nahlásit jakýkoliv bezpečnostní incident. To zahrnuje podezřelé emaily, ztrátu zařízení nebo neoprávněný přístup.

Zálohování

Data uložená na schválených platformách jsou pravidelně zálohována. Uživatel nesmí obcházet tyto mechanismy.

Mobilní zařízení

Mobilní zařízení musí být zabezpečena a registrována v systému správy zařízení. V případě ztráty musí být okamžitě nahlášena.

Práce na dálku

Při práci mimo kancelář je nutné používat VPN a dodržovat stejné bezpečnostní standardy jako v kanceláři.

Kontrola a sankce

Porušení této směrnice může vést k disciplinárním opatřením včetně ukončení pracovního poměru.

Závěr

Dodržování této směrnice je klíčové pro ochranu společnosti TechNova. Každý zaměstnanec je povinen se s ní seznámit a řídit se jí.

IT SMĚRNICE SPOLEČNOSTI TECHNOVA

Úvod

Tato směrnice definuje závazná pravidla pro používání informačních technologií ve společnosti TechNova. Jejím cílem je zajistit bezpečnost, dostupnost a integritu firemních dat a systémů. Směrnice je závazná pro všechny zaměstnance, externí spolupracovníky i dodavatele, kteří mají přístup k IT prostředkům společnosti.

Základní principy

Každý uživatel je odpovědný za bezpečné používání IT prostředků. Přístup k systémům je poskytován pouze v rozsahu nezbytném pro výkon pracovní role. Veškeré aktivity mohou být monitorovány za účelem zajištění bezpečnosti.

Správa hesel

Hesla představují základní bezpečnostní prvek. Je přísně zakázáno hesla sdílet, sdělovat třetím osobám nebo zapisovat na nechráněná místa.

Hesla musí být pravidelně měněna a musí splňovat bezpečnostní požadavky. Doporučuje se používat unikátní hesla pro každý systém.

Používání vícefaktorového ověřování je povinné tam, kde je dostupné.

Ukládání a správa dat

Firemní data musí být ukládána výhradně na schválená úložiště, jako jsou OneDrive a SharePoint. Tato úložiště jsou pravidelně zálohována a splňují bezpečnostní standardy.

Je zakázáno ukládat firemní data na osobní zařízení, externí disky bez schválení nebo na neautorizované cloudové služby.

Sdílení dat mimo organizaci musí být vždy schváleno.

Používání zařízení

Firemní zařízení slouží primárně k pracovním účelům. Každé zařízení musí být zabezpečeno heslem nebo biometrickým prvkem.

Při opuštění pracovního místa je uživatel povinen zařízení uzamknout.

Instalace softwaru

Instalace softwaru podléhá schválení IT oddělení. Používání nelegálního nebo neověřeného softwaru je zakázáno.

Přístup k internetu

Je zakázáno nahrávat firemní data na cizí webové služby, které nejsou schváleny společností.

Používání veřejných WiFi sítí bez VPN je považováno za rizikové.

Bezpečnostní incidenty

Každý zaměstnanec je povinen neprodleně nahlásit jakýkoliv bezpečnostní incident. To zahrnuje podezřelé emaily, ztrátu zařízení nebo neoprávněný přístup.

Zálohování

Data uložená na schválených platformách jsou pravidelně zálohována. Uživatel nesmí obcházet tyto mechanismy.

Mobilní zařízení

Mobilní zařízení musí být zabezpečena a registrována v systému správy zařízení. V případě ztráty musí být okamžitě nahlášena.

Práce na dálku

Při práci mimo kancelář je nutné používat VPN a dodržovat stejné bezpečnostní standardy jako v kanceláři.

Kontrola a sankce

Porušení této směrnice může vést k disciplinárním opatřením včetně ukončení pracovního poměru.

Závěr

Dodržování této směrnice je klíčové pro ochranu společnosti TechNova. Každý zaměstnanec je povinen se s ní seznámit a řídit se jí.

IT SMĚRNICE SPOLEČNOSTI TECHNOVA

Úvod

Tato směrnice definuje závazná pravidla pro používání informačních technologií ve společnosti TechNova. Jejím cílem je zajistit bezpečnost, dostupnost a integritu firemních dat a systémů. Směrnice je závazná pro všechny zaměstnance, externí spolupracovníky i dodavatele, kteří mají přístup k IT prostředkům společnosti.

Základní principy

Každý uživatel je odpovědný za bezpečné používání IT prostředků. Přístup k systémům je poskytován pouze v rozsahu nezbytném pro výkon pracovní role. Veškeré aktivity mohou být monitorovány za účelem zajištění bezpečnosti.

Správa hesel

Hesla představují základní bezpečnostní prvek. Je přísně zakázáno hesla sdílet, sdělovat třetím osobám nebo zapisovat na nechráněná místa.

Hesla musí být pravidelně měněna a musí splňovat bezpečnostní požadavky. Doporučuje se používat unikátní hesla pro každý systém.

Používání vícefaktorového ověřování je povinné tam, kde je dostupné.

Ukládání a správa dat

Firemní data musí být ukládána výhradně na schválená úložiště, jako jsou OneDrive a SharePoint. Tato úložiště jsou pravidelně zálohována a splňují bezpečnostní standardy.

Je zakázáno ukládat firemní data na osobní zařízení, externí disky bez schválení nebo na neautorizované cloudové služby.

Sdílení dat mimo organizaci musí být vždy schváleno.

Používání zařízení

Firemní zařízení slouží primárně k pracovním účelům. Každé zařízení musí být zabezpečeno heslem nebo biometrickým prvkem.

Při opuštění pracovního místa je uživatel povinen zařízení uzamknout.

Instalace softwaru

Instalace softwaru podléhá schválení IT oddělení. Používání nelegálního nebo neověřeného softwaru je zakázáno.

Přístup k internetu

Je zakázáno nahrávat firemní data na cizí webové služby, které nejsou schváleny společností.

Používání veřejných WiFi sítí bez VPN je považováno za rizikové.

Bezpečnostní incidenty

Každý zaměstnanec je povinen neprodleně nahlásit jakýkoliv bezpečnostní incident. To zahrnuje podezřelé emaily, ztrátu zařízení nebo neoprávněný přístup.

Zálohování

Data uložená na schválených platformách jsou pravidelně zálohována. Uživatel nesmí obcházet tyto mechanismy.

Mobilní zařízení

Mobilní zařízení musí být zabezpečena a registrována v systému správy zařízení. V případě ztráty musí být okamžitě nahlášena.

Práce na dálku

Při práci mimo kancelář je nutné používat VPN a dodržovat stejné bezpečnostní standardy jako v kanceláři.

Kontrola a sankce

Porušení této směrnice může vést k disciplinárním opatřením včetně ukončení pracovního poměru.

Závěr

Dodržování této směrnice je klíčové pro ochranu společnosti TechNova. Každý zaměstnanec je povinen se s ní seznámit a řídit se jí.

IT SMĚRNICE SPOLEČNOSTI TECHNOVA

Úvod

Tato směrnice definuje závazná pravidla pro používání informačních technologií ve společnosti TechNova. Jejím cílem je zajistit bezpečnost, dostupnost a integritu firemních dat a systémů. Směrnice je závazná pro všechny zaměstnance, externí spolupracovníky i dodavatele, kteří mají přístup k IT prostředkům společnosti.

Základní principy

Každý uživatel je odpovědný za bezpečné používání IT prostředků. Přístup k systémům je poskytován pouze v rozsahu nezbytném pro výkon pracovní role. Veškeré aktivity mohou být monitorovány za účelem zajištění bezpečnosti.

Správa hesel

Hesla představují základní bezpečnostní prvek. Je přísně zakázáno hesla sdílet, sdělovat třetím osobám nebo zapisovat na nechráněná místa.

Hesla musí být pravidelně měněna a musí splňovat bezpečnostní požadavky. Doporučuje se používat unikátní hesla pro každý systém.

Používání vícefaktorového ověřování je povinné tam, kde je dostupné.

Ukládání a správa dat

Firemní data musí být ukládána výhradně na schválená úložiště, jako jsou OneDrive a SharePoint. Tato úložiště jsou pravidelně zálohována a splňují bezpečnostní standardy.

Je zakázáno ukládat firemní data na osobní zařízení, externí disky bez schválení nebo na neautorizované cloudové služby.

Sdílení dat mimo organizaci musí být vždy schváleno.

Používání zařízení

Firemní zařízení slouží primárně k pracovním účelům. Každé zařízení musí být zabezpečeno heslem nebo biometrickým prvkem.

Při opuštění pracovního místa je uživatel povinen zařízení uzamknout.

Instalace softwaru

Instalace softwaru podléhá schválení IT oddělení. Používání nelegálního nebo neověřeného softwaru je zakázáno.

Přístup k internetu

Je zakázáno nahrávat firemní data na cizí webové služby, které nejsou schváleny společností.

Používání veřejných WiFi sítí bez VPN je považováno za rizikové.

Bezpečnostní incidenty

Každý zaměstnanec je povinen neprodleně nahlásit jakýkoliv bezpečnostní incident. To zahrnuje podezřelé emaily, ztrátu zařízení nebo neoprávněný přístup.

Zálohování

Data uložená na schválených platformách jsou pravidelně zálohována. Uživatel nesmí obcházet tyto mechanismy.

Mobilní zařízení

Mobilní zařízení musí být zabezpečena a registrována v systému správy zařízení. V případě ztráty musí být okamžitě nahlášena.

Práce na dálku

Při práci mimo kancelář je nutné používat VPN a dodržovat stejné bezpečnostní standardy jako v kanceláři.

Kontrola a sankce

Porušení této směrnice může vést k disciplinárním opatřením včetně ukončení pracovního poměru.

Závěr

Dodržování této směrnice je klíčové pro ochranu společnosti TechNova. Každý zaměstnanec je povinen se s ní seznámit a řídit se jí.