	Ingangsdatum: 1 augustus 2011	Laatste datum van herziening: 6 november 2003
	Goedgekeurd door: Compliance-commissie voor senior management	
	Pagina 1 van 5	
Functie: WERELDWIJD BELEID VOOR ELECTRONISCHE COMMUNICATIE		

BEREIK:

Dit wereldwijde beleid voor elektronische communicatie is van toepassing op medewerkers op alle vestigingen van TriMas Corporation en haar dochterondernemingen (gezamenlijk, het 'bedrijf'), evenals adviseurs, aannemers en andere gerelateerde derden die in opdracht bij het bedrijf werken (gezamenlijk 'gebruikers') die goedkeuring hebben voor toegang tot bepaalde systemen die zijn geïnstalleerd, voorzien door en/of eigendom van het bedrijfs ('bedrijfssystemen'). Dit beleid kan op elk moment wanneer dit nodig wordt geacht worden gewijzigd naar eigen goeddunken van het bedrijf. Indien enige bepaling van dit beleid in strijd is met de lokale wetgeving van enig rechtsgebied met betrekking tot bepaalde gebruikers, is deze bepaling niet op gebruikers binnen die jurisdictie van toepassing.

DOEL:

Het bedrijf is afhankelijk van een verscheidenheid aan elektronische media en informatiebronnen om de communicatie tussen de gebruikers te verbeteren en om haar activiteiten te ondersteunen. Het bedrijf geeft gebruikers toegang tot bedrijfssystemen om hun baan of opdracht uit te voeren. Als voorwaarde voor de toegang tot bedrijfssystemen moeten gebruiker zich aan dit beleid houden.


Bedrijfssystemen omvatten, maar zijn niet beperkt tot:

- e-mail, voicemail, Sms'jes, toegang tot internet
- telefoons, mobiele telefoons, iPad's, iPod's en andere draadloze apparatuur
- desktop- en laptop-computers en de softwareprogramma's hiervan
- computernetwerken, inclusief hardware, software en media voor opslag
- faxapparaten, kopieerapparaten, scanners, en elektronische sleutelhangers en kaarten

Gebruikers hebben ook persoonlijke toegang tot elektronische media die onafhankelijk zijn van het bedrijf ('sociale media'). Hoewel sociale media een effectief instrument kunnen zijn voor het delen van ideeën en uitwisselen van informatie, moeten ze worden gebruikt op een manier die de identiteit, integriteit en reputatie van het bedrijfsmerk beschermt. Voor deze doeleinden is het gebruik van sociale media door een gebruiker onderworpen aan bepaalde regels van dit beleid. Deze regels zijn niet bedoeld om het gebruik van sociale media dat geen verband houdt met het bedrijf of bedrijfssystemen te beperken.

Sociale media omvatten, maar zijn niet beperkt tot:

- sites voor professioneel en sociaal netwerken
- blogs en micro-blogs
- discussieforums, chatrooms, on-line forums, markt-websites en andere gedeelde websites
- persoonlijke websites en instant messaging
- enige andere openbare beschikbare communicatiewebsite die via het internet toegankelijk is

	Ingangsdatum: 1 augustus 2011	Laatste datum van herziening: 6 november 2003
	Goedgekeurd door: Compliance-commissie voor senior management	
	Pagina 2 van 5	
Functie: WERELDWIJD BELEID VOOR ELECTRONISCHE COMMUNICATIE		

BELEID:


Het bedrijf bepaalt, naar eigen goeddunken, welk bedrijfssystemen aan een gebruiker ter beschikking staan, en kan vereisen dat een gebruiker één of meer overeenkomsten ondertekent met betrekking tot specifieke bepalingen en voorwaarden met betrekking tot het gebruik van bedrijfssystemen. Toegang tot en gebruik van bedrijfssystemen, evenals het gebruik door medewerker van Sociale Media als het gerelateerd is aan het bedrijf, is onderworpen aan de volgende voorwaarden (die van tijd tot tijd door TriMas kunnen worden gewijzigd):

TOEGESTAAN GEBRUIK:

1. Bedrijfssystemen worden gebruikt voor legitieme zakelijke doeleinden
2. Persoonlijk gebruik van bedrijfssystemen en Sociale Media dat incidenteel is en af en toe voorkomt is toegestaan, zolang het niet storend is voor gebruikers om hun taak uit te voeren of niet door dit beleid verboden wordt
3. Gebruikers mogen alleen de bedrijfssystemen gebruiken waarvoor zij voorafgaande toestemming van het bedrijf hebben ontvangen

VERBODEN GEBRUIK:

1. Uitzending, ontvangst, of weergave van seksueel expliciete informatie, afbeeldingen en berichten, en enige communicatie die kan worden opgevat als discriminerend, beledigend, intimiderend, storend, lastigvallen of kleineren van werknemers, klanten of andere aan het bedrijf gelieerde personen
2. Ongeoorloofde bekendmaking van vertrouwelijke informatie, bedrijfseigendom, handelsgeheimen, of niet-openbare financiële informatie van het bedrijf aan een derde of aan een persoonlijke e-mail account
3. Plaatsen van onjuiste of lasterlijke informatie over het bedrijf, medewerkers, klanten of aan het bedrijf gelieerde personen of communiceren van verklaringen via sociale media die op een verkeerde manier kunnen worden begrepen zodat ze schade kunnen toebrengen aan de bedrijfsreputatie van het bedrijf
4. Schending van de veiligheidsmaatregelen van het bedrijf, met inbegrip van, maar niet beperkt tot, het gebruik van e-mail van een andere gebruiker of ongeautoriseerde toegang tot het netwerk van een individu of een bedrijf
5. Verspreiding, kopiëren of afdrucken van auteursrechtelijk beschermd materiaal, inclusief artikelen en software, hetgeen het auteursrecht schendt


	Ingangsdatum: 1 augustus 2011	Laatste datum van herziening: 6 november 2003
	Goedgekeurd door: Compliance-commissie voor senior management	
	Pagina 3 van 5	
Functie: WERELDWIJD BELEID VOOR ELECTRONISCHE COMMUNICATIE		

6. Zoeken naar religieuze, persoonlijke of politieke zaken op bedrijfssystemen
7. Bedrieglijk voorstellen van een identiteit, met inbegrip van het verzenden van communicatie vanaf de computer van een andere gebruiker of een ander apparaat om uzelf als die gebruiker voor te stellen
8. Zonder toestemming toegang krijgen tot bestanden of communicatie, inclusief het lezen van een mededeling of document bedoeld voor een andere ontvanger
9. Het downloaden of opladen van software van of op bedrijfssystemen zonder goedkeuring van de IT-afdeling van het bedrijf (Let op: Gebruikers moeten alle virussen op bedrijfssystemen aan hun IT-manager rapporteren.)
10. Gebruik van persoonlijke hardware gerelateerd aan bedrijfssystemen
11. Het verzenden van ongecodeerde bestanden met niet-openbare, bedrijfseigen en/of persoonlijke gevoelige informatie met betrekking tot medewerkers van het bedrijf, klanten of aan het bedrijf gelieerde personen zonder toestemming van het bedrijf
12. Het verzenden van ongevraagde e-mails met reclame of marketing in naam van het bedrijf zonder toestemming van de juridische afdeling
13. Om illegale activiteiten te bevorderen of te ondersteunen
14. Het gebruik van bedrijfssystemen na beëindiging van arbeidsovereenkomst of contractuele afspraak, of naar aanleiding van een specifiek verzoek van het bedrijf om het gebruik van bedrijfssystemen te staken
15. Het gebruik van het e-mailadres van het bedrijf om zonder toestemming in te schrijven voor een sociale media-site
16. Het gebruik van bedrijfslogo's of handelsmerken op sociale media zonder voorafgaande schriftelijke toestemming

Als u vragen heeft over wat als een verboden of toegestaan gebruik wordt beschouwd, neem dan contact op met uw leidinggevende of uw lokale (of van uw bedrijf) IT manager, manager personeelszaken of de juridische afdeling.


Andere regels voor het gebruik van bedrijfssystemen en sociale media:

- **Wachtwoorden en beveiliging:** Gebruikers moeten persoonlijke, vertrouwelijke wachtwoorden en toegewezen of persoonlijke ID's gebruiken voor verschillende bedrijfssystemen als methode van

	Ingangsdatum: 1 augustus 2011	Laatste datum van herziening: 6 november 2003
	Goedgekeurd door: Compliance-commissie voor senior management	
	Pagina 4 van 5	
Functie: WERELDWIJD BELEID VOOR ELECTRONISCHE COMMUNICATIE		

authenticatie en controle. Gebruikers zijn verantwoordelijk voor het vertrouwelijk en veilig houden van deze informatie. U mag deze ID's en wachtwoorden aan niemand bekendmaken. Gebruikers zijn verantwoordelijk voor de beveiliging van hun computerterminals. Bij het verlaten van een terminal zonder toezicht of bij het verlaten van het kantoor moeten gebruikers ervoor zorgen dat ze hun terminal blokkeren of zich afmelden om te voorkomen dat niet-geautoriseerde gebruikers toegang krijgen tot het systeem tijdens hun afwezigheid. Gebruikers die een draagbaar apparaat voor communicatie hebben ontvangen, moeten ervoor zorgen dat het te allen tijde veilig wordt bewaard, in het bijzonder tijdens reizen.

- Identificatie op sociale media: Gebruikers die zichzelf identificeren als in dienst zijnde van of die in enig opzicht verband houden met het bedrijf of die bedrijfsgerelateerde zaken on-line bespreken, moeten een clause omvatten waarin staat dat de uitgesproken standpunten die van de auteur zijn en de mening van het bedrijf niet weergeven. U dient er ook voor zorgen dat uw profiel en alle inhoud die u plaatst in overeenstemming is met de professionele uitstraling die u aan klanten en collega's presenteert. Gebruikers zijn zelf verantwoordelijk voor wat ze in sociale media communiceren. Vergeet niet dat wat u publiceert voor lange tijd door iedereen gelezen kan worden (met inbegrip van het bedrijf, toekomstige werkgevers en sociale kennissen). Hou dit in gedachten voordat u inhoud publiceert.
- Controle: Gebruikers zouden geen verwachting moeten hebben van privacy met betrekking tot enig bericht, bestand, enige gegevens, enig document, fax, telefoongesprek, op sociale media gepost gesprek of bericht, of enige andere vorm van informatie of communicatie uitgezonden aan, ontvangen of afgedrukt vanaf, of opgeslagen of opgenomen op bedrijfssystemen. Omdat zowel de systemen als de communicatie erop eigendom zijn van of gelicenseerd zijn door het bedrijf, heeft het bedrijf te allen tijde om zakelijke redenen recht op toegang, doorzoeken, inspecteren, kopiëren en openbaar maken van elk bericht, alle mededelingen of bestanden opgeslagen op bedrijfssystemen, om te voldoen aan alle wettelijke verplichtingen met inbegrip van haar verplichtingen als werkgever en aan de naleving van dit beleid. Het bedrijf kan gebruik van internet ook volgen op gebruiker, met inbegrip van bezochte sites en de frequentie van gebruik, voor zover nodig voor de naleving van dit beleid.
- E-mail protocol: Wees voorzichtig met wat u in een e-mail schrijft. Vraag uzelf af of u zich comfortabel zou voelen als de e-mail gepubliceerd zou worden of als het door een jury gelezen zou worden. Stuur geen e-mail door die door dit beleid wordt verboden, zelf als u het bericht niet gegenereerd heeft. Lees geen e-mail die per ongeluk aan u is verstuurd. Stuur geen junk of massa e-mail en stuur dit niet door vanaf bedrijfssystemen. Alle e-mails van het bedrijf moeten een clause hebben waarin staat dat het bericht alleen bedoeld is voor de ontvanger en dat het vertrouwelijk is.
- Verantwoordelijkheid voor apparatuur: Apparatuur die door het bedrijf aan een gebruiker is verstrekt, is een apparaat zoals gedefinieerd als een bedrijfssysteem op grond van dit beleid, en de gebruiker is verplicht om deze apparatuur op een veilige manier te onderhouden om schade te voorkomen.

	Ingangsdatum: 1 augustus 2011	Laatste datum van herziening: 6 november 2003
	Goedgekeurd door: Compliance-commissie voor senior management	
	Pagina 5 van 5	
Functie: WERELDWIJD BELEID VOOR ELECTRONISCHE COMMUNICATIE		

Apparatuur verstrekt aan de gebruikers blijft te allen tijde eigendom van het bedrijf en moet als zodanig worden behandeld. Gebruikers zullen alle apparatuur bij beëindiging van de arbeidsovereenkomst of het contract of op uitdrukkelijk verzoek van de Vennootschap inleveren. Als een gebruiker schade toebrengt aan de apparatuur of de apparatuur niet zoals vereist inlevert, kan het bedrijf de kosten van de apparatuur incasseren door looninhouding of incasso. Als een recht om de bedrijfssystemen te gebruiken, gaan gebruikers ermee akkoord de vereiste documenten te ondertekenen met betrekking tot het vermogen van het bedrijf om deze kosten terug krijgen.

- **Bewaren van documenten:** Gebruikers moeten voldoen aan alle vereisten voor bewaring van documenten, zoals vereist door het beleid voor bewaren van documenten van het bedrijf met betrekking tot communicatie en documenten die op de bedrijfssystemen zijn opgeslagen, omdat dergelijk beleid van tijd tot tijd kan worden gewijzigd. Gebruikers moeten communicatie en documenten op bedrijfssystemen verwijderen, zoals vereist, tenzij onderworpen aan wettelijke uitstel. Als er wettelijk uitstel is, is vernietiging verboden totdat het tegendeel wordt gemeld. Sla geen documenten of communicatie op verwijderbare apparaten op in strijd met de bewaarperiode van een document. Let erop dat communicatie via e-mail door het bedrijf wordt ondersteund zoals vereist door het beleid voor bewaren van documenten.

Rapporteren van overtredingen

Het is de individuele verantwoordelijkheid van iedere gebruiker dit beleid strikt na te leven. Elke gebruiker die een schending van dit beleid verdenkt of zich hiervan bewust wordt, moet de overtreding aan zijn of haar supervisor, personeelszaken, IT of juridische afdeling melden.

Resultaten van overtredingen

Elke werknemer die in strijd handelt met een wet op elektronische communicatie, een bepaling van dit beleid of enig ander beleid van het bedrijf door het gebruik van sociale media of bedrijfssystemen, met inbegrip van, maar niet beperkt tot, het beleid voor vertrouwelijke informatie en toewijzing van uitvindingen en de Ethische code van zakelijk gedrag, zullen worden onderworpen aan disciplinaire maatregelen, tot en met beëindiging van het dienstverband. Gebruikers kunnen aansprakelijk worden gesteld voor eventuele kosten voor het bedrijf voor ongeoorloofd gebruik van bedrijfssystemen. In bepaalde gevallen kan misbruik van bedrijfssystemen een strafbaar feit zijn.

Voor gebruikers in de V.S.: Dit beleid zal niet worden uitgelegd of toegepast op enige manier die strijdig is met het recht van een werknemer om deel te nemen in beschermde activiteiten, zoals communicatie om lonen, uitkeringen of de arbeidsomstandigheden te verbeteren, zoals bepaald op grond van artikel 7 van de National Labor Relations Act.