A Special Report
Policies and Codes of Conduct for the Use of Social Networks
Leveraging the Benefits, Avoiding the Pitfalls
Policies and Codes of Conduct
for the Use of Social Networks

Leveraging the Benefits,
Avoiding the Pitfalls

Developed by:
E-Business Steering Group
Aerospace Industries Association, Inc.
**Important Disclaimer:** The Aerospace Industries Association of America, Inc. ("AIA") has no intellectual property or other interest in this document. By developing this document and making it freely available to anyone, AIA assumes no responsibility for this Use-case scenario’s content or use, and disclaims any potential liability associated therewith.
# Table of Contents

**TABLE OF CONTENTS** ................................................................. II

**EXECUTIVE SUMMARY** ......................................................... 1

- Background .............................................................................. 1
- Social networking .................................................................... 1
- Key considerations .............................................................. 2

**INTRODUCTION: WHAT IS SOCIAL NETWORKING?** .......... 3

- The Impact of Social Networks ................................................ 3
- Opportunities .......................................................................... 4
- Threats .................................................................................... 5

**KEY RECOMMENDATIONS** .................................................. 9

- A&D company private networking ......................................... 9
  - Policy .................................................................................. 9
  - Code of conduct ............................................................... 10
  - Other key components ..................................................... 10

- Community social networking ............................................. 11
  - Policy ................................................................................ 11
  - Code of conduct ............................................................... 12
  - Other key components ..................................................... 13

- Public social networking .................................................... 13
  - Policy .............................................................................. 14
  - Code of conduct ............................................................... 14
  - Other key components ..................................................... 15

- Further actions ...................................................................... 15

**TEMPLATE SOCIAL NETWORKING POLICY** ....................... 16
Executive Summary

Background
The traditional information technology (IT) environment in companies of all sizes often comprises a controlled set of selected hardware, software and services to deliver integration and economies of scale. Links between companies are achieved through either individually tailored solutions or flexible standards-based interfaces to provide flexibility. These services may be outsourced to third-party providers.

This model is challenged by a range of new technologies and services, characterized by the availability of cheap, powerful consumer devices, virtualization of storage and processors and Internet connectivity.

The nature of the aerospace and defense business implies that the industry is one of the most severe test cases for the effective deployment of such technologies, since it also must support the requirements for export control, intellectual property rights (IPR) protection and national security, such as classified and controlled unclassified information.

In 2010, AIA published an initial statement of the likely impact of these technologies and the business, technical, cultural, operational and security implications for our industry, with the claimed benefits, risks and mitigations. This report, “Disruptive Information Technologies,” [http://www.aia-aerospace.org/assets/report_ebiz_2010_web.pdf] concluded that there are business advantages to utilizing new technologies such as cloud computing and social networking, provided that appropriate precautions are taken to mitigate the risks. Few of these risks are new – or specific to the technologies – but the capabilities of the new technologies serve to exacerbate those risks. The proposed mitigations should be based on the assessment of the corresponding risks within individual organizations.

In 2011, AIA recommended outlines for the policies and codes of conduct that companies should apply to their employees’ use of social networking tools, depending on whether those tools are hosted in a private, community or public environment. The recommendations were based on best practices from member companies at that time.

In the last year, there have been a number of significant developments in the use of social networking, which have driven this rapidly enhancing technology into more mainstream use and permit better management of the risks and benefits from its exploitation to deliver business advantage. They also allow more specific recommendations for industry to be made in this report, along with a template policy and code of conduct for social networking.

Social networking
The social networking phenomenon has been accelerating as a way for individuals to communicate across the industry and to support industry-wide project collaboration. It is the method of choice for the new generation of engineers that we seek to attract into the
industry who are used to open services such as Facebook, and more professional networks like LinkedIn. Most of the services are operated in the cloud environment, with the associated risks and mitigations increasing as the services become more open. The use of in-house systems similar to those available to the public also poses a risk even though they are behind the firewall. The protection of proprietary information that is available to all staff is problematic and should be supported by industry standard security protocols and procedures.

**Key considerations**

The risks arising from social networking do not differ significantly from any other form of interaction between the members of an organization and external communities, but they can be exacerbated by the use of the technology, which can accelerate misinformation and leave permanent records which may be right or wrong.

The risks can be mitigated by a combination of policies and operational constraints, imposed by technical means where appropriate. The extent of mitigation required should be assessed by individual organizations against the risks highlighted in the report, depending on the domain in which they are operating. Such assessments may result in anything from outright banning of access through individual permissions to unlimited connectivity.

In any case, organizations will need to recognize that their employees as individuals may also wish to create, maintain and participate in external social networking tools and websites. The policies established by organizations will need to ensure that the organizations are sufficiently protected where such use can be attributed to the organization, whether directly or indirectly.

This report defines the key issues to be addressed when considering the use of social networking tools within an organization, in a controlled community and in a public environment. Inevitably, the constraints required to protect the organization become more onerous as the environment becomes more public.

The recommended content of policies and codes of conduct for the use of social media should ideally be integrated with existing policies and codes of conduct related to computer usage and network access.

It is also recommended that a community-level collaborative workspace or wiki be established in the AIA Member Connect environment to facilitate the exchange of experiences and best practices.
Introduction: What is social networking?
A social network service focuses on the building and reflecting of social networks or social relations among people (e.g., those who share interests and/or activities). A social network service (also known as one of the defining capabilities of “Web 2.0”) essentially consists of a representation of each user (often a profile); their social links to other people, organizations and events; and a variety of additional services for communicating, playing, sharing and discovering. Most social network services are web-based and provide means for users to interact over the Internet, such as e-mail and instant messaging. Although online community services are sometimes considered as a social network service in a broader sense, a social network service usually means an individual-centered service whereas online community services are group-centered.

Social networks can be established in domains that are restricted to the whole or part of an organization, to a community of interest across multiple organizations or completely open to the public. It is also possible to establish social network services “behind the firewall,” now commonly referred to as “Enterprise 2.0.”

Social networking is recognized as a disruptive IT component in an organization, since it offers new, spontaneous, ungoverned and uncontrolled capabilities to acquire and synthesize information in an innovative manner.

Most social networking services external to an organization operate in a cloud environment, independent of location, so all the risks and mitigations for the various classes of cloud-based services also apply to social networking. The specific requirements of the aerospace and defense industry demand particular care, since proprietary information is not only business critical but can be a national security risk if exposed inappropriately.

Industry considers that the technology is widespread and pervasive; the AIA eBusiness Steering Group is seeking to provide some authoritative guidance on how these services can be used to deliver benefit without compromising businesses or their security.

The Impact of Social Networks
A number of key events and changes have precipitated consideration of social networking as a disruptive technology for the traditional computing environment in the aerospace industry. The availability of tools such as Facebook and LinkedIn has generated a new expectation for accessing information from people in an individual’s network, which may extend outside a single organization. This needs to be balanced with the need to recognize the restrictions of export control, IPR and copyright.

Since the publication of the previous recommendations in 2011, a number of further trends have emerged which increase the impact on the aerospace and defense industry as social networking capabilities transition from disruptive technology to mainstream business.
• New recruits to the industry are attuned to the opportunities arising from a community approach to solving problems and gathering information, which need to be balanced with effective restraints related to IPR, export control and national security. The decision by DOD to permit the use of social networks by military personnel subject to particular operational constraints provides another impetus for broader use of the technology.

• More companies are deploying social networking capabilities internal to their own environment and are experiencing improved information flow and better access to enterprise expertise, although there is a risk of work disruption for individual experts as others have instant access to them. Appropriately controlled, this may drive up the overall productivity of the organization.

• Company experience of the use of social networking is increasing, allowing more refined assessment of the risks and benefits and opening the way to managed exploitation with broader recognition of the risks of compromising data.

• Technological controls over web access are now available at a more granular level, allowing the company to restrict individuals to viewing but not posting content, mitigating some of the risks

• The new category of Controlled Unclassified Information opens up a new range of sensitive information which needs to be considered in setting policies related to social media. It has been observed that such information can appear to be available in the public domain, even if it is not supposed to be released, as the amount of information in this category is substantial, and leaks are more likely.

**Opportunities**

Social networking provides a number of opportunities to improve the productivity of a company by connecting people with each other and to make more information available when and where it is needed.

• For example, some companies are using social networking technologies within their own domain to help employees gain access to subject matter experts, build internal communities of interest/practice and facilitate knowledge sharing between retiring workers and their successors. By making the senior members of an organization more visible and available, the technology can flatten organizational hierarchies, enhance knowledge workers’ productivity and improve overall business agility.

• Social networking opens up a two-way channel between a company and its customers to share ideas, feedback and even deliver customer services

• A social networking tool can pull discussions and debates out of people’s e-mail in-boxes and make the information visible to anyone on the networking service, not only
in a particular group or to the whole company. This kind of visibility can facilitate “viral” innovation, improving the speed of information flow and/or branding, but risks data spill if the domain extends beyond the company.

- Public social networks can be used to attract and recruit the talent a company needs and to draw in new customers. A vibrant social network around a company can make it attractive to new recruits and help them to integrate. With careful management, trade associations and companies can use networks as a powerful marketing tool for their products and other messages. Industry can also observe such networks to track public perception of a company, using sentiment analysis tools.

- Public and community social networks can be used to discuss topics that are relevant to communities of interest/practice that include people from different organizations, companies or even countries. For example, the AIA REACH-IT wiki is a collaborative tool for sharing and building information on this important piece of European legislation, offering companies the opportunity to exchange knowledge and save costs.

- A social network can become a treasure chest of organizational knowledge that can be reused in any number of ways. For example, technologies such as mashups (composition of web services or composite applications) can leverage a social network to combine the information stored there to discover new insights or to form new teams to address a particular need. The same openness can be exploited by the service provider to synthesize information – this is generally part of their business model. As an example, Facebook will compare the lists of friends of individuals and offer suggestions to expand the network.

**Threats**

As noted above, all the risks and mitigations associated with private, community and public clouds apply to social networking services operating in those environments.

Since the purpose of social networks is to make people and information visible, there are a number of risks that come with using them. It must be emphasized that these risks are not unique to social networking, although the technology can increase the level of risk.

Below is a table of risks and recommended mitigation strategies to address them. Internal networks are synonymous with private implementations and external networks may be community or public.
### Risks

Sensitive or classified information may be posted on internal or external social networks, making it visible to those who are not authorized to view it and creating a liability to the company through violations of security, export control, insider trading and IPR restrictions. There are also implications for eDiscovery in litigation, particularly for material exposed on external networks.

### Mitigations

- Establish policies for your company on what information can and cannot be shared on internal social networks and on external networks. Provide that policy to the company employees and make it visible to them when they enter social networking sites.
- Include in the policy a clear definition of who can access external networks from the workplace and for what purpose. Enforce the access policy using automated controls.
- For internal social networks, provide a capability to tag information as sensitive and to limit who can view information that has a “sensitive” tag on it.
- For internal social networks, determine if you can provide sufficient controls to protect export-controlled information from being shared or stored in violation of export control laws. If you cannot, forbid export-controlled information from being posted to the site.
- Establish “spill response” procedures for addressing the cleanup of unauthorized sharing of sensitive information.
- Classified information should never be posted to any kind of social network.
- Ensure that company material is protected by copyright.
<table>
<thead>
<tr>
<th>Risks</th>
<th>Mitigations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employees may speak on behalf of the company when they are not</td>
<td>• Designate who can speak on behalf of the company.</td>
</tr>
<tr>
<td>authorized to do so, sharing information that is not fully</td>
<td>• Require others to include a “personal opinion” disclaimer on their posts</td>
</tr>
<tr>
<td>accurate or not consistent with company policies or branding.</td>
<td>to social networks and to avoid making statements about company policies or</td>
</tr>
<tr>
<td></td>
<td>plans.</td>
</tr>
<tr>
<td></td>
<td>• Monitor key social networking channels for violations</td>
</tr>
<tr>
<td></td>
<td>• Configure web proxies to permit read-only access</td>
</tr>
<tr>
<td>People can post false information, defame your people or company or</td>
<td>• Employ image or brand management techniques – regularly search for your</td>
</tr>
<tr>
<td>do other damage to your company’s brand or reputation.</td>
<td>company’s name on social network sites respond appropriately to information</td>
</tr>
<tr>
<td></td>
<td>that is damaging, either through dialogue or through having it removed</td>
</tr>
<tr>
<td></td>
<td>from the site by the administrators. It should be noted that sometimes it</td>
</tr>
<tr>
<td></td>
<td>is better to ignore items rather than grant credibility through responding.</td>
</tr>
<tr>
<td>“Hactivism” applied via social networking can lead to account</td>
<td>• Careful monitoring of channels</td>
</tr>
<tr>
<td>spoofing and denial-of-service attacks</td>
<td>• Consider limiting participation to sites that have strong responses to</td>
</tr>
<tr>
<td></td>
<td>spoofing and other misuse</td>
</tr>
<tr>
<td>Social networks may reduce productivity for some employees. For</td>
<td>• Establish and communicate clear policies on appropriate use of social</td>
</tr>
<tr>
<td>example, senior employees and subject matter experts may lose</td>
<td>networks, providing guidance on etiquette, time charging and “response</td>
</tr>
<tr>
<td>control of some of their time because they are more available to</td>
<td>time” expectations.</td>
</tr>
<tr>
<td>others. Some employees may spend too much time responding to the</td>
<td>• Focus on efficiency gains and specific success stories to allay the</td>
</tr>
<tr>
<td>latest discussion post and there is always the risk of social</td>
<td>fears of senior management that key individuals are being diverted from</td>
</tr>
<tr>
<td>networking intrusively interrupting workflow.</td>
<td>projects.</td>
</tr>
<tr>
<td></td>
<td>• Establish and communicate clear policies on appropriate use of social</td>
</tr>
<tr>
<td></td>
<td>networks, providing guidance on etiquette, time charging and “response</td>
</tr>
<tr>
<td></td>
<td>time” expectations.</td>
</tr>
<tr>
<td></td>
<td>• Focus on efficiency gains and specific success stories to allay the</td>
</tr>
<tr>
<td></td>
<td>fears of senior management that key individuals are being diverted from</td>
</tr>
<tr>
<td></td>
<td>projects.</td>
</tr>
</tbody>
</table>
### Risks

Social networking can enable the aggregation of previously unlinked information – social networking sites are designed to facilitate this. There may also be a question as to who owns the IPR of the result, since there is no contractual environment.

Intelligence gathering by collection and collation of data can unintentionally expose company structures and plans, such as acquisition targets and supplier preferences.

Collation of personal data from multiple sites can allow malicious hackers to assemble a profile of individuals and their families, which can be used to more accurately tailor malware and spoof emails, opening up new attack vectors for APT on companies.

Uncontrolled use of external sites may absorb significant network bandwidth.

Access to external sites risks the interaction and intermingling of personal and business transactions and information.

### Mitigations

- Establish policies for your company on what can and cannot be shared on internal social networks and on external networks.
- Provide that policy to the company employees and make it visible to them when they enter social networking sites.
- Move discussions to less public environments.

- Establish policies for your company on what can and cannot be shared on external social networks.

- Provide advice for employees about what should not be shared on social networks.
- Provide regular training updates on how to avoid inadvertent compromises of the network, at home or at work.

- Establish and communicate clear policies on appropriate use of social networks, providing guidance on etiquette, time charging and “response time” expectations.
- Consider restricting access to high-bandwidth sites.

- Establish policies for your company on what can and cannot be shared on external social networks.
- Provide that policy to the company employees and make it visible to them when they enter social networking sites.

In any case, companies will need to recognize that their employees as individuals may wish to create, maintain and participate in external social networking tools such as blogs, wikis, chatrooms, podcasts, microblogging such as Twitter and discussion boards. They may also participate as individuals in social websites such as Facebook, LinkedIn and other online activities.
In order to minimize the risk of data exfiltration or reputation damage to the business, it is advisable to minimize the overlap between business and personal social networking, although it is becoming increasingly difficult for individuals to protect their business identities from their private identities, due to the use of tools to correlate data from different sources.

**KEY RECOMMENDATIONS**

The use of social networking tools can undoubtedly bring increased agility and capabilities to access and synthesize information within an organization, across a community or beyond. The increasingly pervasive nature of the technology implies that all organizations, irrespective of their size, need to address the issue.

The risks arising from social networking do not differ significantly from any other form of interaction among the members of an organization and external communities, but can be exacerbated by the use of the technology.

The risks can be mitigated by a combination of policies and operational constraints, imposed by technical means where appropriate. The extent of mitigation required should be assessed by individual organizations against the risks highlighted above, depending on the domain in which they are operating. Such assessments may result in anything from outright banning of access through managed individual permissions to unlimited connectivity.

The recommended content of policies and codes of conduct for the use of social media should ideally be integrated with existing policies and codes of conduct related to computer usage and network access.

**A&D company private networking**

Organizations operating a social network within their own IT domain should implement the following components to mitigate risk. Users should be aware that internal users can view all content posted on the social networking site, and might read it without any necessary supporting context.

**Policy**

Policy statements should:

- Define the objectives for the use of the service, such as information exchange, collection and dissemination of tacit knowledge, and collaborative development of solutions;
- Define any restrictions on access to the service;
- Provide guidance on ownership of content by the organization;
- Provide rules related to discussion and posting of protectively marked material, covering at least controlled unclassified information, national security, export control and proprietary data:
For national security marked material, users should not discuss or post material unless they can be completely sure that all participants in the network and the service provider have necessary clearances. Classified material should never be posted.

For controlled unclassified information (CUI), users should not discuss, post or proliferate any CUI material, even if it appears to be available in the public domain, unless they can be completely sure that all participants in the network are eligible to see such items.

For export control marked material, users should not discuss or post material unless they can be completely sure that all participants in the network are eligible to see such items.

For proprietary data, it is assumed that participants in the internal network will be permitted to view such information, unless there are additional restrictions applied.

Personal information protected by US federal, state, local or international laws and regulations should never be shared.

It is recommended that an explicit list of protective markings that either can or cannot be discussed on the network is provided.

- Provide a process for removing inaccurate, inappropriate or objectionable content, or material that is in conflict with the policy and code of conduct;
- Define organization rights related to the governance of content, including removal of any material that it may require;
- Ensure that employees assume all legal liability that may result from their postings;
- Specify that organization equipment should be used in compliance with any existing acceptable use policy;
- Define organization sanctions that may be applied for misuse of the network.

Code of conduct

The code of conduct should cover:

- Expected behaviors and etiquette on the internal social network, including the need to:
  - Treat others with dignity;
  - Respect others’ privacy;
  - Avoid posting material that is defamatory, obscene, profane, threatening, abusive, harassing or targeted toward any person or entity within the organization and its leadership, customers, suppliers and competitors.
- Compliance with applicable laws in any jurisdiction that may have access to the internal network;
- Explicit links to any overarching organization code of conduct.

Other key components

The policy and code of conduct should be supported by actions to:

- Tag information that is controlled by export, security or other restrictions, to reduce the likelihood of inadvertent release;
- Control access to the network by technical means;
• Remind users of their responsibilities when they enter the social networking site;
• Provide the staff with initial training and continuing education on the policy and the code of conduct, as part of regular refresher training;
• Establish a governance function for the service as a focus for monitoring usage and issues, involving representatives from groups responsible for:
  – Security;
  – Legal, including IPR;
  – Human resources;
  – Export/import control;
  – Operations;
  – Ethics; and
  – IT.

The governance function should monitor operation of the service to ensure that it aligns with the defined objectives within the organization, and should have the rights to administer the policy and code of conduct.

**Community social networking**

Organizations using a community social network hosted outside their domain should implement risk mitigation strategies. It is assumed that there are published rules that are applied for defining those who are permitted to join the network, otherwise the network should be treated as a public social network as below. Users should be aware that any users within the community, whether inside their organization or external competitors or customers, can view all content posted on the social networking site, and might read it without any supporting context that may be essential for understanding. Care should also be taken in selecting the network to ensure that the selected network complies with controls on multinational hosting of information.

**Policy**

Policy statements should:
• Define the objectives for the use of the service, such as information exchange, collection and dissemination of tacit knowledge, and collaborative development of solutions;
• Define any restrictions on access to the service, for both reading and posting;
• Provide guidance on ownership of content by the organization in the community environment, recognizing that information created on the network may be jointly owned by all the participating organizations and can be freely exploited by them;
• Provide rules related to discussion and posting of protectively marked material, covering at least controlled unclassified information, national security, export control and proprietary data:
  – For national security marked material, users should not discuss or post material unless they can be completely sure that all participants in the network and the service provider have necessary clearances. Classified material should never be posted.
  – For controlled unclassified information (CUI), users should not discuss, post or proliferate any CUI material, even if it appears to be available in
the public domain, unless they can be completely sure that all participants in the network are eligible to see such items.

– For export control marked material, users should not discuss or post material unless they can be completely sure that all participants in the network are eligible to see such items.

– For proprietary data, it is recommended that only information covered by appropriate NDA/PIA nondisclosure agreements can be shared.

– Personal information protected by US federal, state, local or international laws and regulations should never be shared.

– It is recommended that an explicit list of protective markings that either can or cannot be discussed on the network is provided.

– If in doubt, don’t share!

• Define organization rights related to the governance of content, including removal of any material;

• Provide a process for removing inaccurate, inappropriate or objectionable content, or material that is in conflict with the policy and code of conduct;

• Require employees to state that any views expressed are those of the individual, not of the organization, unless they are explicitly authorized to present an organization view (e.g., corporate communication functions);

• Provide an explicit process for dealing with requests arising from the media by passing them through approved channels to obtain an organization response;

• Ensure that employees assume all legal liability that may result from their postings;

• Specify that organization equipment should be used in compliance with any existing acceptable use policy;

• Define organization sanctions that may be applied for misuse of the network.

**Code of conduct**

The code of conduct should cover:

• Expected behaviors and etiquette on the community social network, including the need to:

  – Treat others with dignity;
  – Respect others’ privacy;
  – Avoid posting material that is defamatory, obscene, profane, threatening, abusive, harassing or targeted toward any person or entity within the organization and its leadership, customers, suppliers and competitors.

• Compliance with applicable laws in any jurisdiction that may have access to the community network;

• Explicit links to any overarching organization code of conduct;

• Appropriate external use, such as avoiding statements on organization policies and plans and material that could represent an anti-trust violation;

• Any restriction on the posting of branded or other organization-generated promotional material;

• Recognition of risks of using external social networking, such as targeting of individual employees, introduction of malicious software into individual
computers and organization networks, and compromising of personal and financial information.

**Other key components**

The policy and code of conduct should be supported by actions to:

- Tag information that is controlled by export, security or other restrictions, to reduce the likelihood of inadvertent release;
- Restrict network access to particular individuals by technical means;
- Remind users of their responsibilities when they enter the social networking site;
- Provide the staff with initial training and continuing education on the policy and the code of conduct, as part of regular refresher training;
- Establish a governance function for the service as a focus for monitoring usage and issues, involving representatives from groups responsible for:
  - Security;
  - Legal, including IPR;
  - Human resources;
  - Export/import control;
  - Operations;
  - Ethics; and
  - IT.

The governance function should monitor operation of the service to ensure that it aligns with the defined objectives within the organization and should have the rights to administer the policy and code of conduct. They should also be responsible for managing “data spills” from the organization by taking the necessary actions to remove or mitigate the effects of a spill.

**Public social networking**

Organizations using a public social network hosted outside their domain should implement the following components to mitigate risk.

It should be recognized that individuals using a public social network from within an organization can be linked to the organization, in the same way that they could associate themselves with the organization from a private computer. Even if they are working as an individual from a private computer, there is a risk that they can be associated with the organization.

Users should be aware that any other users of the network – whether inside their organization or external competitors or customers, news media or those engaged in espionage – can view all content posted on the social networking site, read it without any supporting context that may be essential for understanding and use it for any purpose.
Policy

Policy statements should:
- Ensure that the policy applies whenever an individual can be associated with the organization, whether or not they are using organization or private equipment;
- Define the objectives for the use of public services, such as information exchange, collection and dissemination of tacit knowledge and collaborative development of solutions;
- Define any restrictions on access to individual services from organization resources, for both reading and posting;
- Provide guidance on any ownership of content by the organization in the public environment, recognizing that information created on the network may be jointly owned by all the participants and can be freely exploited by them;
- Prohibit the discussion and posting of protectively marked material, covering at least controlled unclassified information, national security, export control and proprietary data;
  - Provide an explicit list of protective markings that either can or cannot be discussed on the network is provided.
  - If in doubt, don’t share!
- Define organization rights related to the governance of content, including removal of any material;
- Provide a process for removing inaccurate, inappropriate or objectionable content, or material that is in conflict with the policy and code of conduct;
- Where an employee’s comments can be attributed to the organization, require employees to state that any views expressed are those of the individual, not of the organization, unless they are explicitly authorized to present an organization view (e.g., corporate communication functions);
- Provide an explicit process for dealing with requests arising from the media by passing them through approved channels to obtain an organization response;
- Provide the organization with the right to monitor employee postings on public social networking sites, whether originating from organization or private equipment;
- Ensure that employees assume all legal liability that may result from their postings;
- Specify that organization equipment should be used in compliance with any existing acceptable use policy;
- Define organization sanctions that may be applied for misuse of public social networking sites.

Code of conduct

The code of conduct should cover:
- Expected behaviors and etiquette on the public social network, including the need to:
  - Treat others with dignity;
  - Respect others’ privacy;
– Avoid posting material that is defamatory, obscene, profane, threatening, abusive, harassing or targeted toward any person or entity within the organization and its leadership, its customers, suppliers and competitors.

- Compliance with applicable laws in any jurisdiction that may have access to the network;
- Explicit links to any overarching organization code of conduct;
- Appropriate external use, such as avoiding statements on organization policies and plans and material that could represent an anti-trust violation;
- Any restriction on the posting of branded or other organization-generated promotional material;
- Recognition of risks of using external social networking, such as targeting of individual employees, introduction of malicious software into individual computers and organization networks, and compromising of personal and financial information.

**Other key components**

The policy and code of conduct should be supported by actions to:

- Tag information that is controlled by export, security or other restrictions, to reduce the likelihood of inadvertent release;
- Restrict network access to particular individuals by technical means;
- Remind users of their responsibilities when they enter the social networking site;
- Provide the staff with initial training and continuing education on the policy and the code of conduct, as part of regular refresher training;
- Establish a governance function for the service as a focus for monitoring usage and issues, involving representatives from groups responsible for:
  - Security;
  - Legal, including IPR;
  - Human resources;
  - Export/import control;
  - Operations;
  - Ethics; and
  - IT.

The governance function should monitor usage of social networking services to ensure that they align with the defined objectives within the organization and should have the rights to administer the policy and code of conduct. They should also be responsible for managing “data spills” from the organization, taking the necessary actions to remove or mitigate the effects of a spill.

**Further actions**

As the capabilities and technology related to social networking continue to evolve, there will be an ongoing need for companies to share their best practices and experiences. It is therefore recommended that a collaborative document or a Wiki be set up on the AIA MemberConnect service to act as a repository for current requirements and templates for policies.
Template Social Networking Policy

This policy covers the most open use of social networking in a public environment, and its provisions may be restricted in cases where there is no use of public social networking sites. Job titles and controlled lists such as classification schemes may be tailored as required.

1.0 Policy

It is the policy of Company XYZ to permit the use of Social Networking services in accordance with this guidance in order to inform, communicate and engage with all of our stakeholders. Company XYZ recognizes that these types of communication platforms can support the successful operations of the Company when properly used in accordance with Company policies and applicable laws.

2.0 PURPOSE

This policy and associated guidelines for the use of Social Networking have been established to ensure that these communications channels are used appropriately for business purposes and to reduce the risk of inappropriate disclosure of information belonging to Company XYZ and its customers and suppliers, minimize the risk of malware infection and lessen the exposure to social engineering threats. Together, these documents also set forth the requirements and expectations regarding the posting in Social Networks of any information or content related to Company XYZ, whether in a business or personal capacity.

3.0 APPLICABILITY AND SCOPE

This guidance applies to all employees and contractors of Company XYZ. This policy can be changed at any time by Company XYZ in its sole discretion. It is neither intended to nor does it create any contractual relationship between an employee or contractor and Company XYZ. Once printed or duplicated, this policy is not a controlled document. The most up-to-date version of the policy exists in electronic form on the Corporate Policy web site.

4.0 DEFINITIONS

4.1 Social Networking - Social Networking covers social interaction on the internet, including the dissemination of content created using highly accessible and scalable publishing techniques. Examples include Internet Forums, Blogs, Chat Rooms, Wikis, Podcasts, Twitter, Mashups, Facebook, Linkedin, MySpace, Plaxo, Jigsaw, Orkut, Nexopia, Bebo and You Tube.

4.2 Protectively Marked - Documents that have been designated as requiring special handling by Company XYZ, governmental authorities or pursuant to agreements with third parties. Examples include: Company Private, Competition Sensitive, Controlled Unclassified, Proprietary Information, Commercial in Secret, Trade Secret, Confidential, Secret and Top Secret.

5.0 REQUIREMENTS

5.1 Official Company Social Networking Sites. Official Company Social Networking sites are those that are established by Communications Department personnel for the purpose of communicating Company information to external audiences. These sites are primarily designed to promote Company XYZ's products, services and capabilities to key audiences and online communities. All official Company Social Networking sites must be approved, in advance, by Communications. These sites are controlled by Communications and only authorized representatives in Communications may post approved digital content and information to them. Additional guidance regarding official company Social Networking sites can be found in Appendix A to this policy "Guidelines for Communications' Use of Social Networking."

5.2 Business Use of Social Networking. Employees and contractors are permitted to use Social Networking sites for specific Company purposes. Some examples of business use include: business development, business communications, training and market research. When using
Social Media sites for business purposes, employees may only post or share information that has previously been approved for public release by Communications, such as news releases, electronic brochures or marketing materials, or other approved digital content and text.

5.2.1 Approval process. When preparing posts for business use of Social Networking, employees and contractors should contact the Communications staff and seek approval prior to posting any content.

5.3 Personal Use of Social Networking. All personal use of Company information technology resources, including for Social Networking purposes, is subject to all applicable Company policies, including, for example, Company XYZ Policy, "Acceptable Use of Information Resources." Please note that the Company reserves the right to monitor all activity using Company assets for Social Networking purposes. Regardless of whether Company information technology is used, employees and contractors who post to Social Networking sites for personal purposes are personally responsible for such postings. Employees and contractors should use restraint and consider the risk to customers, Company XYZ, other employees and themselves. Any and all information posted to the internet can instantaneously become global in nature. Detailed guidance for employees and contractors who choose to use Social Networking sites for personal purposes is found in Company XYZ Social Networking Policy Guidance Appendix B, "Guidelines for Employees' Use of Social Networking Tools."

5.4 Employment or Business References. Employees and contractors are prohibited from using Social Networking to provide references or recommendations for current or former employees or contractors.

5.5 Prohibited Information. To maintain and protect the Company's reputation, employees and contractors are prohibited from posting information or content of the following types or topics:

5.5.1 Any information or content that is misleading or otherwise untrue. In particular, any communications about the Company's customers, competitors, potential competitors, suppliers, current employees or former employees should be carefully reviewed.

5.5.2 Confidential internal memos.

5.5.3 Documents that have been protectively marked (or any abstract thereof).

5.5.4 Confidential information or content, whether Protectively Marked or not, belonging or related to the Company or belonging or related to clients, customers, partners, vendors or suppliers, including but not limited to the identity of same, without permission. This includes non-public corporate or financial information or content, including but not limited to forward looking guidance, revenue projections, earnings, future product launch details, acquisition or divestiture activity, customer wins, or relationships with customers or partners.

5.5.5 Classified, Controlled Unclassified or export controlled information.

5.5.6 Intellectual property belonging to Company XYZ or others such as technical data, ideas, inventions, software, copyrighted material, etc.

5.5.7 Personally identifiable information about an individual including but not limited to personal data and images, employee travel plans, business itineraries, personal health and financial information unless the individual has provided prior permission for such use of the information.

5.6 External Social Networking Sites. External social networking sites are frequently used for information harvesting, spyware and malware distribution. Examples of malicious activity include:
Employees and contractors should protect the Company and themselves by not opening media attachments from unknown sources and by regularly participating in required IT security awareness training.

5.7 Compliance With Applicable Laws and Policies. At all times, an employee's or contractor's use of Social Networking must be in compliance with this policy and all other Company policies, the Company XYZ Code of Conduct and other applicable laws, regulations and policies of the location in which the employee or contractor is employed or engaged. The Company will not construe or apply this Policy or associated guidance in a manner that interferes with or infringes on employees' rights under Section 7 of the National Labor Relations Act to communicate with others about wages, hours or other terms and conditions of employment or to otherwise engage in protected, concerted activity.

6.0 RESPONSIBILITIES
The Senior Vice President, Communications is the custodian of the policy and is responsible for its administration and for associated guidance. Employees and contractors are responsible for following the policy and associated guidance.

7.0 EXCEPTIONS
Exceptions to this policy require the prior written approval of the President of Company XYZ or the Senior Vice President, Communications.
Appendix A

Guidelines for Communications Use of Social Networking Tools

The following guidelines describe the process and procedures that govern how Company XYZ Communications will use official Company XYZ Social Networking sites such as Facebook, Twitter, YouTube, Flickr, blog sites, etc.

These guidelines are intended to outline official company use of Social Networking tools. At all times, all Company XYZ employees are required to act ethically and it is every employee’s obligation to review and understand the Code of Conduct, the Communications policy and confidentiality obligations in other relevant policies.

At all times, Company XYZ employees must be in compliance with the Company XYZ Code of Conduct and the federal, state and/or local laws and regulations of the location in which they are employed or engaged.

Communications Use of Social Networking Tools

Official company information is distributed to external audiences by Company XYZ Communications staff or official company spokespersons. Communications will use Social Networking tools to communicate and engage with key audiences and the communities of users who choose to join or follow Company XYZ’s activities on the company’s official Social Networking sites.

Official Social Networking sites are those that are set up by Communications personnel for the purpose of communicating digital content. Communications personnel in Company XYZ’s business sectors and business units must receive prior approval from the Director of Digital Communications for Company XYZ. Communications will set up any external Social Networking site. For sites or accounts established prior to the publication of these Guidelines, the site owners must notify Communications to continue using the site.

Company XYZ’s official Social Networking sites are primarily designed to promote Company XYZ’s products, service and capabilities to key audiences and online communities. For example, when information and digital content are released to the public via a news release or media distribution service, this content will also be posted to the Company’s external website, www.companyXYZ.com, as well as the Company XYZ Twitter account and/or other relevant Social Networking sites. Information posted to Social Networking sites by Communications staff will be approved in accordance with Company XYZ Policy, Corporate Communications and Public Information, prior to external release. Depending on the nature of the digital content, the review could include, but is not limited to, export control, legal, security and select business leaders consistent with Policy.

Company XYZ Communications personnel will maintain monitoring capabilities to track public comments posted to Company XYZ’s official Social Networking sites. If information is requested from Company XYZ through a Social Networking site by an audience or online community member engaging in social dialogue, only information that has been approved for external release will be sent in response to such a query.
Communications Governance of Social Networking Tools
Each business sector will designate a management-level Communications executive responsible for coordinating their respective digital media activities and managing of the requirements of this policy guidance.

This designee will work in coordination with Company XYZ Communications on all Social Networking activities undertaken by the respective sector. The designee will participate in a Social Networking training session focused on understanding the best industry Social Networking practices and reducing the risk of inappropriate disclosure of Company XYZ information. This session must be completed before access to post content is provided on any of Company XYZ’s official Social Networking sites and/or before any requests to create new sites are granted.

Each business sector will prepare a weekly report highlighting Social Networking activity on sites maintained within that sector and its respective business areas.

Only Communications personnel may use “Company XYZ” in any URL, Twitter hashtag, YouTube, other video site channels, etc. The use of “Company XYZ” in any URL, Twitter hashtag, YouTube or other video site channel, etc., must be approved by Company XYZ Communications. This is to ensure the brand is not compromised as well as to make clear what information is coming from the Company and what information is coming from private individuals.
Appendix B

Guidelines for Employees' Use of Social Networking Tools

All employees should exercise caution and good judgment about statements made online. If you choose to communicate via Social Networking channels in your personal capacity, whether you use Company XYZ services and resources or not, we suggest that you follow the common sense guidelines set forth below.

Please note that the Company reserves the right to monitor all activity using company assets for Social Media purposes if you use Company XYZ resources or services to communicate online, whether for business purposes or personal purposes and whether at work or on your personal time.

In addition, you are expected to comply with the federal, state and/or local laws and regulations of the location in which you are employed or engaged. Employees outside the U.S. should consult their local policies for guidance.

The Company will not construe or apply this Guidance or the associated Policy in a manner that interferes with or infringes on employees' rights under Section 7 of the National Labor Relations Act to communicate with others about wages, hours, or other terms and conditions of employment or to otherwise engage in protected, concerted activity.

GUIDELINES

1. Setting Up Personal Spaces in Social Networking Channels. Company XYZ employees may establish an online presence and use Social Media platforms including blogs and microblogs (Facebook, LinkedIn, Twitter, etc). Employees who establish these personal sites may not use "Company XYZ" or any version of "Company XYZ" in any part of the name or URL of the site so as to avoid confusion with official Company XYZ communications. If you use any information that comments on your status with Company XYZ, we recommend you have a clear disclaimer highlighting that this is not an official Company XYZ site. Remember that you are personally responsible for everything you publish on-line. Template: "The views expressed in this (blog, microblog, website, etc.) are my personal views and do not in any way constitute official Company XYZ positions, policies or endorsements."

NOTE: Managers and Executives: The above disclaimer does not by itself exempt managers and executives from a special responsibility when commenting or communicating online, regardless of the communication platform. Due to their position, managers and executives must be aware that whatever they publish online could be misconstrued to be an official Company XYZ policy and/or position. Further, managers and executives need to be aware that any public online communication could be seen and read by Company XYZ employees and that Social Media is not the appropriate forum for internal deliberations.

2. Write in the first person. Be sure you are speaking only for yourself; i.e., use the first person singular, such as "I believe ..." and not "Company XYZ believes ..." Remember that only Corporate Communications or a designated spokesperson may speak officially for Company XYZ.

3. Be Truthful and Respectful. Tell the truth and if you find you have made a mistake, issue a prompt clarification or a withdrawal. Your behavior on-line should be consistent with the Company's Code of Conduct and policies.

4. Don't Pick Fights. Contact Company XYZ Communications staff if/when you see misrepresentations or false statements about Company XYZ by bloggers, the media, analysts or anyone else. Do not engage in the point-counterpoint of blogging or discussion forums on Company-related issues. Leave that to Company Communications professionals.
5. **Do Not Post Anything that Would Not Be Acceptable in the Workplace or that Is Unlawful.** You should not post any content that is or could be construed as discriminatory, bullying, intimidating, harassing, threatening or pornographic. You must uphold the Company’s value of respect for the individual at all times. Do not make negative, disparaging, discriminatory, or defamatory statements about the Company, the Company’s employees, customers, vendor partners or others, including its competitors. Do not use ethnic slurs, personal insults, obscenity or engage in any conduct that would not be acceptable in the workplace. Show proper consideration for topics that may be considered objectionable or inflammatory – such as politics or religion.

6. **Protect Everyone’s Privacy.** The internet provides a sense of anonymity, and the lack of face-to-face communications can lead to a false sense of security. You should never disclose personal information such as addresses, telephone numbers or information about schedules or daily routines, either your own or anyone else’s. It is a good idea to limit the amount of personal information you post.

7. **Using Photographs and Videos.** Be considerate when posting photographs or videos online. If they contain images of other employees or friends, ask yourself if they would be comfortable with you posting their images. Not everyone is willing to have their likeness posted on the internet. Remember, even if you remove a photograph from a site it is likely to be cached or saved on other sites. You should also comply with company rules concerning photographs taken on company premises and the use of images from company sites, taking account of copyright.

8. **Friends and Strangers.** The internet makes it easy for people to disguise their identity. Don’t invite people into your online network or to be a “friend” until you are comfortable they are being honest with you.

9. **Legal Considerations.** The rules surrounding copyrighted material and other intellectual property, export control, security classification, fair use and financial disclosure laws and discussion of Company XYZ business arrangements in general still apply. Do not discuss any confidential information, including information regarding any possible future or current business deal or future products, revenue projections or targeted acquisitions. If you are unsure of whether to post certain information, do not post it. If you have any questions, please contact your local Communications staff.

10. **Social Computing and Your Primary Role.** Be aware that having an active online presence can be time consuming, so it is important that this does not interfere with your role at Company XYZ. Note that any Social Media activity you engage in after normal working hours can also have an impact on the Company, so these Guidelines and the applicable policies apply.