Based on the article written by SunMicrosystem’s Joel Weise and Charles R. Martin in “Developing a Security Policy”, this paper would first explain the concept of an information policy in an organizational perspective. Then, it would show how Internet-based activities in organizations could be limited accordingly.

The foundation for information policy research (FIPR) defines information policy as an interaction between technology and society. Their goals as they have stated in their website is to “promote public understanding and dialogue between technologists and policy makers in the UK and Europe” (FIPR). Both of these notations show how modern this concept of ‘information policy’ is in this new era of the ‘Internet’. In addition to that, the foundation has five basic fields in which they categorized their specialty in promoting laws and regulations in societies; they are classified as follows:

- Trust in e-commerce and e-governance
- Surveillance and Security
- Intellectual Property and the Public Domain
- International Law and the Internet
- Academic Freedom

All these fields are considered not very new to world’s societies, yet considered by many that they cover the Internet-based activities as a whole. Many do not notice that laws concerning the Internet differentiate enormously from the civil and commercial laws practiced since ages.

For the trust in e-commerce and e-governance matter, the foundation gave an example regarding the electronic voting that occurred in the United States year 2000. The main topic aroused was the disputed Florida ballot, where it is claimed that the system was not handled in a much secured way. Electronic commerce and electronic governance systems are made to provide a simplified administration and a better service plus a relatively reduced cost and for some systems also, to ‘control fraud’. That is the main purpose behind integrated IT/IS systems in organizations. So, returning to the electronic voting issue, which could be classified under this e-governance concept, the technological and information control infrastructure was ‘supposed’ to handle the system’s information flow in a positive way, but, by naming the effects, it didn’t!! So, the issue now is who is responsible? Is it the designers and developers of the system, or the
people whom the system was done for, or is it the technology, or are they the hackers who caused all this chaos? To add to this question, the foundation has proposed two perceptions, which are the ideas of two individuals strongly related to this field. One, Dr Rebecca Mercuri (FIPR), a world leading researcher on e-voting, stated that “it is not presently (nor in the foreseeable future) possible to construct a secure, Internet-based system for remote electronic voting…” this has been stated before the elections took place, as if to warn the organization concerned with this matter. Then one of the designers and developers of the GNU.FREE Internet Voting System also stated “over the past 3 years, it has become clear that creating an Internet Voting System sufficiently secure, reliable and anonymous is extremely difficult if not impossible”. Note that both statements made have severely doubted the possibility of administrating an online based system, both from individuals with high status in this field, of whom words could be taken with seriousness, yet it did not. And it was still hard to hold someone the responsibility for what happened.

Surveillance and Security are two related issues in the Internet Information Policy. Anyone may notice how very strict security standards have been implemented, especially after the September 11 attacks on the US government, which was and would always be the start of an era in public surveillance, where anyone would be suspected for terror and organized crime. Thus, perfect national security intelligence would always be aimed at by all governments who expect an attack somehow by unidentified individuals who may not even commit a crime for a reason, but to exploit ideas and beliefs or just for the sake of hatred, which would eventually be overpowered by revenge. Since then, and some information under specific attitudes may be banned from public view, for the reason that they may hold violence-promoting ideas. Similar trends of information may also be used as ‘bates’ for surveillance as if to check out who goes out online browsing for information that, to the government officials, may hold violence against them. As a conclusion to this point, people may be spied at by government officials, under the justification that they are ‘maintaining national security’.

Very similar to this field is the Intellectual Property against the Public Domain, where privacy acts and copyright policies over the Web Domain are looked after. To be defined easier, copyright policies over the Internet is what is happening with peer to peer
file sharing engines like Kazaa, Napster, Limewire, E-Mule, and so on till the never-ending story!! All the matter is should these source files that are shared are to be treated as tangible property? So should they have the protections of tangible property? Or should these pieces of ‘information’ be seen as a common resource as they are not depleted when shared? (FIPR) Such information when provided online, they do not hold any cost except the space they take, which is fairly ‘cheap’ to conduct. Although the many anti-piracy promotions been made on TV commercials and all mediums of advertisement, societies as are yet merely convinced that doing such acts is ‘by law AND morals’ is considered or ‘supposed’ to be considered unethical/illegal. Until these days, not all laws in governments or authorities that maintain policies are legible. One issue that stands out against this is globalization of the Internet (part of the Int’l Law and the Internet); that is treating the Internet as one world, thus holding one common rule in any particular matter. Governments hold agreements and understandings through the World Trade Organization but with no complete resolutions for this sake.

Secondly are the Privacy policies. The foundation revealed acts regarding privacy in the health industry. In the National Health Service (NHS), due to the very weak security controls and also the privacy mechanisms that are not yet defined properly, 200,00 attempts have been every year they say (FIPR), through health authorities who hold patients’ details, made ‘illegally/immorally’ by investigators who call up pretending to be doctors or administrators. The solution is very easy, the foundation responses, which is to provide encrypted data that defines every patient without having the initials every where, especially with in the hands of people who do not know how to respond to such situations. The justification has always been, as the foundation also says, by holding responsibility to the system itself as being not 100% efficient and secure. This opens again the topic of trust in e-governance.

At the end, through an organization-wide perception, developing a security policy in an organization would be very difficult without defining first what information policy is as a nation-wide perspective and then, those policies cannot be implemented if the government(s) concerned have yet not deployed a policy that stands out with, not against, both private and public domains.
References:

  Retrieved at 19-10-05

  http://www.ingentaconnect.com/content/pal/0960085x/2001/00000010/0000001/3000372
  Retrieved at 13-10-05

  Retrieved at 12-10-05