



Ipsos Information Security Policy

Date: **December 2010**

By **Dr. Ben Booth – Chief Information Officer**
John van Loenen – Global Information Security Director



Contents

Introduction	3
Part 1: Ipsos User Information Security Policies	4
Information Handling Policy	4
Computer Acceptable Use Policy	6
Password Policy	7
PDA/Smartphone Policy	8
Remote Access Policy.....	9
Part 2: Information Security Awareness	10
Your Laptop, PC and Mobile Devices	10
Physical Security	12
Virus Protection	13
Spyware/Malware.....	14
Social Engineering/Phishing	16



Introduction

Dear Ipsos Colleagues,

The attached documents set forth Ipsos' policies and procedures with respect to data protection and information security.

As technology rapidly advances, and our access to information increases greatly, we are presented with many new challenges with respect to how we protect and manage our data. Our clients are also placing increasing pressure on us to assure them that we have sufficient procedures in place to guarantee the safety and security of their data at all times.

Protecting Ipsos' and our client's data is a monumental task and can only be done with the co-operation of all Ipsos employees at every level. Understanding how to better protect our data through Information Security Awareness and complying with User policies that help protect this data is imperative.

It is the responsibility of our country managers, IT managers and HR managers to implement these policies and ensure that every employee and other user of our systems (such as consultants and vendors/suppliers) receive and understand them. Most importantly, all employees will be expected to adhere to these policies and best practices. Failure to comply with this policy may lead to disciplinary sanctions.

Dr. Ben Booth
Chief Information Officer

John van Loenen
Global Information Security Director



Part 1: Ipsos User Information Security Policies

Information Handling Policy

Purpose: The purpose of this document is:

1. to define Security Sensitive Information that Ipsos employees may have access to
2. to provide instruction on the safe access, storage and control of Security Sensitive Information
3. to provide instruction on the safe transmission of Security Sensitive Information, and;
4. to provide instruction on the procedure to follow in the event of loss of company provided equipment and materials containing Security Sensitive Information.

Security Sensitive Information:

Personally Identifiable Information (PII): refers to information that can be used, independently or together with other information, to uniquely identify, contact, or locate a single individual. Examples include name, age, gender, mailing address, phone numbers, email address and identification numbers (for example, Social Security Numbers and Social Insurance Numbers). Typically we are sent PII information that includes a full name and contact information (such as an e-mail address or telephone number) from our clients.

Sensitive Personal Information: This includes data about an individual's racial or ethnic origin, age, date of birth, political opinions, religious beliefs (or other beliefs of a similar nature), physical or mental health, sexual life/sexuality, financial information (bank account number, credit scores, income, salary, bonus, Ipsos Financial Data etc) and criminal proceedings or convictions. For Ipsos employees, typically, the only people in possession of this data are Human Resource, Finance staff and department head staff. We may also receive this sort of information with respect to survey respondents.

Client Information: refers to all information that may identify a client and is protected under a non-disclosure agreement. Examples of such information may include, without limitation, contracts, research presentations and results, briefs, Ad Tests, and any client information contained in proposals, questionnaires and screeners.

Company Confidential Information: refers to all Ipsos owned information such as financial reports, trade secrets, mergers and acquisitions, strategies etc.

Access, Storage and Control of Security Sensitive Information:

- Only those employees who are directly authorized to work on a project/task and handle Security Sensitive Information may do so.
- Employees may only access Security Sensitive Information if it is strictly necessary in connection with their job responsibilities.
- Security Sensitive Information can only be stored on an Ipsos owned or controlled server with appropriate logical access controls in place.
- Security Sensitive Information cannot be copied to any storage media (USB hard drives, memory sticks, etc.) or computers (home PCs, etc.) that are not Ipsos owned.
- Any Security Sensitive Information stored on any Ipsos owned laptop, PC, CD's, DVD's, portable hard drive, USB key and hard disk must have whole-disk encryption installed. This includes laptops with Security Sensitive Information stored as e-mail attachments.
- PII and Sensitive Personal Information may only be used for the purposes identified to the individual when it was collected, and may not be used or disclosed for any other purpose, unless required by law.
- PII or Sensitive Personal Information cannot be modified or altered for any unlawful purposes.



Transmission of Security Sensitive Information to an Ipsos Client:

- E-mail and ftp (File Transfer Protocol) are not allowed to be used for the purpose of transmitting PII and Sensitive Personal Information outside of Ipsos. For the transmission of Client Sensitive Information, please refer to the Master Service Agreement or NDA for the client.
- SFTP (Secure File Transfer Protocol) and HTTPS (Secure HTTP) are permitted for transferring Security Sensitive Information.
- Encryption of the file attachment may be required dependant on client requirements.
- An agreement must be in place to ensure the confidentiality and security of the Security Sensitive Information that is being transferred.
- Note that PII and Sensitive Personal Information collected by Ipsos may only be shared with a client in limited circumstances for valid research purposes. Please consult with your local Privacy Officer and Legal department for guidance in a particular instance.
- It is extremely rare that extensive PII and Sensitive Personal Information is provided by a client. Always verify the sample the client is providing you is not in excess of what we require to complete the study.

Transmission of Security Sensitive Information to an Ipsos Vendor/Supplier:

- The exact same level of security used with the client must be used with the vendor/supplier. No exceptions.
- Security Sensitive Information that is provided to us by a client should only be disclosed to a vendor/supplier with the consent of the client.
- **An agreement must be in place with the vendor/supplier to ensure the confidentiality and security of the Security Sensitive Information that is being transferred.**

Reporting

- Legislation in various regions and our Master Service Agreements with our clients typically obligate us to report any loss of Security Sensitive Information.
- Security Sensitive Information can be contained on company owned devices and property such as laptops, PC's, Blackberry's, CD's, DVD's, portable hard drives, USB keys, paper and hard disks.
- Any loss or unauthorized access to Security Sensitive Information must be reported **immediately:**
 - **To your local IT Service Desk**
 - To the Global Director of Information Security – global_security@ipsos.com
 - On weekends and bank holidays 1-516-247-1880.
 - The failure to promptly report such loss or unauthorized access may result in disciplinary action.
- In addition, the following steps must be taken in coordination with the Global Information Security team:
 - File a police report. Obtain a Police Report Number and, if possible, investigating officer name and badge number.
 - File a Lost and Found report (if applicable) and obtain a reference number, or person's name, business card, etc.
 - Be prepared to assist the Information Security team in completing the incident report.



Computer Acceptable Use Policy

Employees are expected to use company provided internet access, e-mail, computers, servers, mobile devices (cell phone, BlackBerry etc) electronic media (disk, CD-ROM, DVD, USB Data Keys etc) and voice and voicemail systems for business purposes. Users are permitted access to the Internet and electronic communication systems to assist in the performance of their jobs.

Personal use means use that is not job related. In general, incidental and occasional personal use of Ipsos' Internet access or electronic communications is permitted; however, personal use is prohibited if it:

- Directly or indirectly relates to personal business (i.e. all activities, non-job related, by which you can obtain a personal gain/benefit) ;
- Interferes with the user's productivity or work performance, or with that of any other employee;
- Adversely affects the efficient operation of our computer systems, networks or the desktop/laptop software.

Because access to such systems is considered a privilege of employment and the systems remain Company property at all times, these systems could be subject to inspection from time to time by Ipsos (when legally permissible) to ensure compliance with this policy and to help ensure the security and protection of our business information.

Certain activities are prohibited when using the Internet or e-mail. These include, but are not limited to:

- Accessing, downloading, printing or storing information with sexually explicit content;
- Downloading or transmitting fraudulent, threatening, obscene, intimidating, defamatory, harassing, discriminatory, or otherwise unlawful messages, files or images;
- Installing or downloading computer software, hardware, programs, or executable files unless approved by your local IT department;
- Installing, downloading, or providing for download by others, any content where copyright law is being violated
- Sending e-mail using another's identify, an assumed name or anonymously.
- Using the company allocated email address to register with non - business web sites or other non business activity that aggravates the reception of spam mail

All staff will use Ipsos Legal approved disclaimers in their e-mails.

Ipsos reserves the right to remove any non-business files or programs stored on company devices.

Any Ipsos employee found in violation of the above policies may be subject to disciplinary action.



Password Policy

To enhance security in our environment, we have established a password policy defining the password length, complexity, reuse of old passwords and frequency of password change.

Password Length:

Your password must be at least eight (8) characters long.

Password complexity:

Your password must use a combination of lowercase, uppercase and numbers so the password cannot easily be guessed by someone trying to break in. Depending on your access rights, you may also be required to include non-alphanumeric characters ("special characters") in your password. See below for the rules you must follow to ensure your password meets minimum requirements.

Password Re-Use:

You cannot re-use a password until after you have changed to a different password 3 times. If you use the default frequency of 3 months between changes, the earliest you would be able to re-use a password is after almost a year, but we recommend you do not re-use them at all.

Frequency of Change:

You must change your password at least every 3 months (90 days). If you connect to the network on a wired connection, you will be prompted to change your password starting 21 days before expiry, however, those who connect remotely, or who always use wireless, will NOT be prompted. In that case, please set a recurring task in Outlook to remind you to change the password before it expires so you don't get locked out.

Password Confidentiality:

User names and passwords are to be considered private, and should not be shared with anyone, either Ipsos employee or non-employee. You are responsible for all activity occurring under your account, regardless of who was actually at the keyboard; if you think your password has been compromised, or have shared it with someone in the past, change it immediately to one only you know and then notify the helpdesk. To further protect your account, lock Windows (press Ctrl-Alt-Del and choose Lock Computer) when you must leave the system logged on and unattended.

If you need access to a resource for which you do not currently have permission, you must call the helpdesk to have access granted to your own account; you may not use someone else's account.

How to create a strong password (for standard user accounts):

Passwords must, as a minimum, contain a mixture of letters AND numbers. In addition it is recommended that you also use a mix of upper case and lower case letters.

Example:

Password you want to use: finewine

Suggested password: F3neW4ne



PDA/Smartphone Policy

Handheld devices such as PDAs (Personal Digital Assistant) and smartphones are both useful business tools and significant security risks. To best protect Ipsos and its clients, the following policy has been put in place.

Supported Devices

1. Only Ipsos-owned and managed devices may be connected to the corporate network, or to its e-mail systems.
2. The RIM BlackBerry is the only generally approved device and is managed by a BlackBerry Enterprise Server.
3. Exceptions may be granted by the senior IT executive in a region if
 - a. Client demands dictate the use of another device (eg: Microsoft requires Windows Mobile devices be used by its account team) **and**
 - b. The device can be centrally managed through the current infrastructure (only Microsoft ActiveSync is currently supported) **and**
 - c. The IT security team has evaluated and approved the device.

Usage Policies

1. Devices may only access Ipsos e-mail through approved channels (eg: the BlackBerry Enterprise Server link, Outlook Mobile Access (OMA) Exchange Servers); corporate e-mail may not be simply forwarded to a device.
2. Devices must be password protected; passwords must be 4 or more characters in length.
3. In the case of the BlackBerry, the standard list of forbidden passwords must be deployed.
4. In the case of devices managed by Microsoft ActiveSync, password complexity must be enabled.
5. The maximum time, in minutes, that elapses before the PDA device locks and prompts the user for the security password: 15 minutes.
6. Devices must be centrally managed, with approved configurations.
7. Access to the Intranet or other internal network resources from a handheld device is not permitted.
8. Lost or stolen devices must be reported to Helpdesk immediately so the command can be sent to securely erase the data from the missing device.



Remote Access Policy

All Ipsos users must use an Ipsos-provided PC and connect to one of the remote access hubs on Ipsos networks for access.

All connections must be connected by creating a VPN (Virtual Private Network) tunnel to one of our remote access hubs with authentication via Cisco access control server.

- All users must be Ipsos employees with user IDs in Ipsos active directory.
- All connecting devices (laptop, desktops) must be imaged by Ipsos.
- When a user is connected to the VPN, all network and Internet traffic must go through the Ipsos network by default. Simultaneous, separate connections to the Internet are not permitted.



Part 2: Information Security Awareness

Your Laptop, PC and Mobile Devices

Ipsos employs various standards to protect information on computers and laptops but be mindful of the following:

- The information on a lost or stolen laptop, PC or USB thumb drive that is not encrypted can still be accessed and read.
- The BIOS password and Windows login password are key to security but can be defeated with time and various utilities.

Incorporate the following into your routine:

- Back up files stored on your laptop to the file server on a regular basis.
- Transfer files off of your laptop when they are no longer required.
- Do not store sensitive data on your laptop or USB drive. If you do, ask the IT department about having your hard drive or device encrypted.
- Secure your laptop with a cable lock during working hours.
- Lock your laptop in a drawer or filing cabinet when not in use or not taken home.
- Never leave your laptop in a vehicle where it is visible. Lock it in the trunk/boot and secure the trunk/boot. An SUV, Pick-up, Van, Mini-Van or Hatchback's storage compartment is not a trunk/boot.
- Not all car trunks/boots can be properly secured. A properly secured car trunk/boot must have a trunk/boot pop latch that can be locked and rear seats that can be locked into place preventing access to the trunk/boot.
- In a hotel, lock your laptop in the room safe (if it is available) or store it out of sight when you are not in your room.
- Airports, train terminals, subway stations, bars are prime areas for laptop theft. Keep your laptop bag near you and never leave it unattended.
- When you are travelling, remember that thieves will often distract you, or wait until you are distracted, before stealing your laptop. When it is not over your shoulder you should always keep your laptop case in sight, and preferably keep one of the straps looped round your arm or leg.
- Position laptops away from people in public places.
- Lock down your PC if you intend to step away from it by pressing – CTRL-ALT-DELETE and pressing "ENTER".
- Immediately pick up confidential jobs from printers and faxes.



- Deposit confidential papers into the shredder or designated shredding bins. Note that documents that are thrown into the trash become part of the public domain. Dumpster Diving is legal! Anyone can look through Ipsos's garbage once it has left our control.



Physical Security

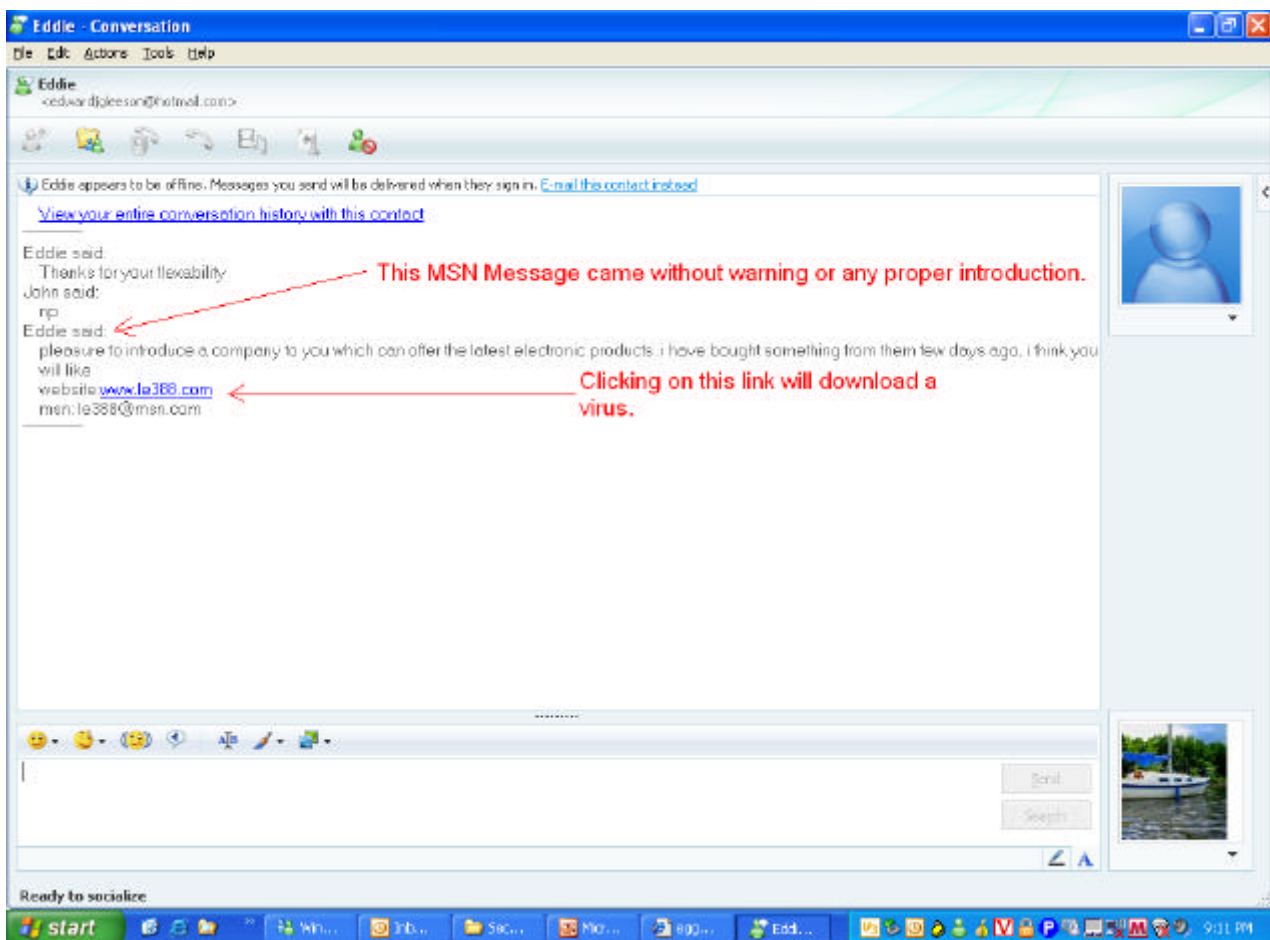
- Do not allow anyone into our premises that you don't know. This is the most common way to breach physical security.
- Challenge anyone who is attempting to gain access to Ipsos premises to produce their swipe card or Ipsos ID.

Virus Protection

A **computer virus** is a computer program that can copy itself and infects a computer. Viruses are propagated primarily through e-mail and by file sharing inside of Instant Messaging.

How do you prevent your PC/Laptop from being infected?

1. Never turn off your anti-virus
2. Be suspicious of unsolicited e-mails from unknown sources
3. Do not open emails if there is a suspicious subject header like "Attention" or "Congratulations, you've just won..." or "Your PC is infected – please click here".
4. Do not click on any links in suspicious Pop-Ups that have messages like "Attention" or "Congratulations, you've just won..." or "Your PC is infected – please click here".



Spyware/Malware

Malware is software designed to secretly access a computer system without the owner's informed consent. Delivery of Malware can be done by visiting a website in what is called a "drive-by download site".

Malware can do the following:

- Install advertising via a pop-up
- Track your web surfing habits
- Capture your keystrokes
- Enlist your PC as a "robot" in a much larger "Bot" army used to attack other systems on the internet. Usually referred to as a Botnet. See illustration on next page.

Spyware/Malware prevention:

- Your browsers (IE and Firefox) have pre-configured security settings – do not change them.
- Try to stay on known or trusted Internet sites.
- Download programs or software only from trusted sites
- Never click on unwanted pop-ups. Shut them down by clicking on the red "X" in the upper right hand corner of the pop-up window.
- Your PC comes with an anti-spyware program – do not disable it.
- Google and other search engines now identify potentially dangerous sites – heed their warning!
- Typical sites that have malware/spyware are online gambling, get rich and porn sites.
- As the example on the next slide indicates, legitimate sites can be hacked and malware/spyware placed on them. This is usually the case if the web server is not regularly patched with the necessary security updates.

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Refresh Print Mail W Yellow E

Address <http://www.google.ca/search?hl=en&q=diesel+engine+manufacturers&meta=>

Links Citrix Portal Customize Links Free Hotmail Webmail Windows Windows Marketplace Windows Media

Web Images Maps News Video Gmail more ▾

Google diesel engine manufacturers Search [Advanced Search](#) [Preferences](#)

Search: ☒ the web ☐ pages from Canada

Web Results 1 - 10 of about 2,620,000 for [diesel engine manufacturers](#).

[Diesel Engine Manufacturers](#)
[This site may harm your computer.](#)
Diesel Engine Manufacturers. The following listings are some of the leading manufacturing companies in the world. Of course, **Diesel Service and Supply** is ...
www.dieselserviceandsupply.com/Diesel_Engine_Manufacturers.aspx - [Similar pages](#)

[Engine Manufacturers Association - About Members](#)
Engine Manufacturers Association ... Detroit **Diesel** Corporation · Deutz Corporation · Dresser Waukesha · Fiat Powertrain Technologies SpA ...
www.enginemanufacturers.org/about_members/ - 11k - [Cached](#) - [Similar pages](#)




[Diesel Engine Manufacturers & Suppliers](#)
Diesel Engine Manufacturers ★ Verified with 3 or more face-to-face visits by Global Sources
 ★ Choose Verified Wholesale **Diesel Engine Manufacturers** ...
www.globalsources.com/manufacturers/Diesel-Engine.html - 140k - [Cached](#) - [Similar pages](#)

[Diesel engines - all the Manufacturers | Industry | Industrial ...](#)
Diesel engines - Find all the industrial **manufacturers** on DirectIndustry | industry ... 6 cylinder turbocharged **diesel engine** Perkins Engines Inc ...
www.directindustry.com/industrial-manufacturer/diesel-engine-62663.html - 142k - [Cached](#) - [Similar pages](#)

[Diesel Engine Suppliers](#)
 The following list of **Diesel engine manufacturers** was taken from the February 1998 National Fisherman magazine. Contact the **manufacturers** for information on

Sponsored Links

[Diesel Engine Directory](#)
Diesel Engine Manufacturer
 The Top Industrial Resource.
Dieselengines.Industrial101.com

start    >> diesel engine manufa...

Google now labels sites that contain malware.

Social Engineering/Phishing

Social Engineering

- Social Engineering: the act of manipulating people into performing actions or divulging confidential information.
- End goal is deception and ultimately a human operator is fooled into removing or weakening system defenses.

Phishing

- The act of sending an email and pretending to be from an online store, a financial institution or an Internet service provider with the intention of gaining personal information from the recipient.
- An e-mail usually claiming that you need to go to click on a link to update your account information.
- The link is “spoofed” or falsified to send you to a “hacker” site that looks and feels like the real site.
- The falsified site steals your credentials

Phishing Prevention

- Never open an e-mail attachment from someone that you don't know.
- Never disclose personal information via e-mail.
- Never disclose client confidential information to a 3rd party unless they are a trusted source authorized to receive the information.

