



## 306 Workplace Privacy

**James R. Beyer**  
*Counsel*  
Accenture

**William Davis Harn**  
*Senior Attorney*  
Southern California Edison Company

**Larry L. Sharrar**  
*General Counsel*  
Lockheed Martin Space Operations

## Faculty Biographies

### James R. Beyer

James R. Beyer is counsel for Accenture, in Chicago and currently serves as the global director of labor relations for the Accenture legal and commercial group. He is responsible for all labor and employment law issues related to the company's more than 110,000 personnel globally. Accenture is a global management consulting, technology services, and outsourcing company.

Prior to joining Accenture, Mr. Beyer was a senior attorney for International Business Machines Corporation. Mr. Beyer was counsel to the law firm of Gardner, Carton & Douglas. He was a senior associate with the law firm of Seyfarth Shaw. He served as a judicial law clerk in the U.S. District Court for the Northern District of Illinois. Mr. Beyer is also an Adjunct Professor at IIT Chicago-Kent College of Law where he teaches Privacy in Employment Law.

Mr. Beyer formed the pro bono legal committee at Accenture and he has been active in pro bono work for the Greater Chicago Food Depository, Community Christian Alternative Academy, United Power for Action and Justice, and the Episcopal Lawyer Volunteer Network.

Mr. Beyer received a B.A. from DePauw University and is a graduate with high honors from the IIT Chicago-Kent College of Law where he was an editor of the Law Review.

### William Davis Harn

William Davis Harn is presently a senior attorney within the employment and benefits law section of the Southern California Edison Company (SCE) law department in Rosemead, California. His practice consists of employment litigation in state and federal courts as well as providing day-to-day advice to management and human resource professionals on a broad spectrum of labor, employment, and benefits related issues.

Before joining SCE, Mr. Harn was an associate with the Los Angeles based national law firm of Sheppard, Mullin, Richter and Hampton. Mr. Harn also worked in corporate and executive level positions in accounting and financial management before beginning his legal career.

Mr. Harn volunteers regularly with the Los Angeles County Superior Court as a mediator, arbitrator, and temporary judge. He is also currently the vice president of his law school's alumni board.

Mr. Harn received his B.S. from the University of California at Davis and his J.D. from the University of the Pacific, McGeorge School of Law.

### Larry L. Sharrar

Larry L. Sharrar is the general counsel for Lockheed Martin Space Operations in Houston, Texas and Lockheed Martin Technical Operations, in Colorado Springs, Colorado. His responsibilities include providing legal counsel to the presidents and senior staffs of both of these dynamic business

units in all areas of operation, managing business unit litigation, and monitoring and documenting compliance with federal, state, and local laws.

Prior to his current assignments, Mr. Sharrar was assistant general counsel for health and safety for the Lockheed Martin Corporation, and before that, an associate general counsel for Lockheed Martin Missiles and Space Company. Mr. Sharrar also served as a judge advocate general in the U.S. Air Force, specializing in government procurement law.

Mr. Sharrar received a B.S. from United States Air Force Academy, an M.S. from the University of Tennessee, and is a graduate of the University of Washington School of Law.



## Session 306: Workplace Privacy

**James R. Beyer**

*Counsel, Accenture*

**William Davis Harn**

*Sr. Attorney, Southern California Edison Company*

**Larry L. Sharrar**

*General Counsel, Lockheed Martin Space Operations*

ACC's 2005 Annual Meeting: Workplace Privacy

October 17-19, Marriott  
Wardman Park Hotel



## Balancing Rights

- Privacy Rights

Right to be secure in person and property

- Management Rights

Right to operate the enterprise

ACC's 2005 Annual Meeting: Workplace Privacy

October 17-19, Marriott Wardman Park Hotel



## Constitutional Protection of Privacy Rights

- U S Constitution/Bill of Rights
  - 1st Amendment
  - 4th Amendment
- State Constitutions
  - e.g. California: Article I, Section 1



## Statutory Safeguards of Workplace Privacy

- HIPAA/ADA/FMLA
- FCRA/Criminal History Inquiries
- Polygraph Laws
- Federal/State Wiretap/Eavesdropping Laws
- ECPA (Interception vs. Stored information)



## Topics for Discussion

- Privacy in the Electronic Workplace
- Privacy of Person, Personal Information and Data
- International & Foreign Issues regarding Privacy

ACC's 2005 Annual Meeting: Workplace Privacy

October 17-19, Marriott Wardman Park Hotel

## Privacy in the Electronic Workplace

Does What Goes on in the Cubicle...  
Stay in the Cubicle?

Larry L.Sharrar  
General Counsel, LMSO

ACC's 2005 Annual Meeting: Workplace Privacy

October 17-19, Marriott Wardman Park Hotel



## Better Living Through Electricity

- Telephone Monitoring.
- E-mail Monitoring.
- Video Monitoring of Work Area.
- Computer Monitoring.
- Monitoring of Personal Websites and Blogs.

ACC's 2005 Annual Meeting: Workplace Privacy

October 17-19, Marriott Wardman Park Hotel



## Scenario

- Dr. Gavin, a long time employee of the company, and a PhD in Software Engineering, maintains an extensive database of Victoria Secrets Catalog pictures on his work computer. The folder is password protected, and contains over 3,000 different photographs. Alerted to the fact that he was not just doing work on his computer, through video monitoring of the workplace. His stash of photos is discovered when the company runs a newly installed search engine that checks all company owned computer databases for illegal or improper software. Although no illegal software was discovered on Dr. Gavin's computer, he was terminated for having pornographic photographs on his work computer.

ACC's 2005 Annual Meeting: Workplace Privacy

October 17-19, Marriott Wardman Park Hotel



## The Issues

- Dr Gavin's expectation of privacy?
  - What is a reasonable expectation?
    - Video Monitoring?
    - Established Company Policies?
- Company's right to search individual computer databases?
  - Ownership rights?
  - Obligation to protect employees and customers?
- What are the limitations on the rights of both Parties?

ACC's 2005 Annual Meeting: Workplace Privacy

October 17-19, Marriott Wardman Park Hotel



## The Employee: Expectation of Privacy

- What is reasonable expectation of privacy in workplace today?
- What can an employee do to protect his/her privacy in the workplace?
- Is there a requirement to notify employees of the actual level of privacy in workplace?

ACC's 2005 Annual Meeting: Workplace Privacy

October 17-19, Marriott Wardman Park Hotel



## The Company: Right to Monitor

- Courts have consistently allowed electronic monitoring in the workplace.
  - What is the workplace?
- The ECPA provides several exceptions for electronic workplace monitoring.
- Policies regarding monitoring must be made known to employees to be effective

## The Future: Where are we going?

- Technology continues to evolve.
- The definition of the “Workplace” continues to evolve.
- Society’s expectation of Privacy continues to evolve.
- Needs v. Wants.





## Guidance On Accessing Stored E-mail

- Essential administrative purpose, or
- Investigative purpose based on reasonable suspicion of work-related misconduct.
- Follow written policies
  - ✓ Voiding expectations of privacy
  - ✓ Educate employees that transmissions are essentially permanent, i.e. **Delete ≠ Delete**
  - ✓ Warnings re monitoring
  - ✓ Limiting and/or prohibiting personal use
  - ✓ Limiting and/or prohibiting unlawful use
- When appropriate obtain consent
- When in doubt seek legal counsel

## Privacy of Medical and Employment Data

### Navigating the Maze of Employee Information

William Davis Harn  
Senior Counsel  
Southern California Edison Company



## REASONABLE EXPECTATION OF PRIVACY

- Can be limited by statute, contract, and notice
- Can be limited by owner's right to control property where private facts may be placed or private activity may occur.
  - Should be exercised for legitimate business purpose only
  - How would you like it if ...

ACC's 2005 Annual Meeting: Workplace Privacy

October 17-19, Marriott Wardman Park Hotel



## Disclosure of Employment Information

- Disciplinary records, compensation/position history, performance evals, personal data, pension information, etc.
- To the Employee?
- To persons other than Employee?
  - Spouses? Significant Others? (ERISA)
  - Unions? (29 USC 158(a)(5); 440 US 301)
  - Prospective employers? (defamation risks)
  - Co-workers? (110 Cal.App. 4<sup>th</sup> 180)
- Mandatory Disclosures
- Social Security Numbers

ACC's 2005 Annual Meeting: Workplace Privacy

October 17-19, Marriott Wardman Park Hotel



## WHAT IF ... (Hypo No. 2)

- Manager comes to you for advice. Employee has come to Manager complaining about a negative performance evaluation given to her by Supervisor, Manager's direct report. Employee claims that Supervisor shared the performance review with all employees in a staff meeting. Employee also claims that co-employees have refused to cooperate with her on work assignments and have made unjustified complaints about her to their supervisor in retaliation for her having told the supervisor that a co-employee's expense report was inappropriate. Employee is now out 'sick', has submitted doctor's notes saying that she is suffering from 'stress', and has demanded to be transferred to another business unit. Employee also tells Manager she has reported the expense report issue to the Audits Hot Line and she will report it to public regulatory authorities if the Company does not address it. What is your advice?

ACC's 2005 Annual Meeting: Workplace Privacy

October 17-19, Marriott Wardman Park Hotel



## WHAT IF ... (Hypo No. 2)

- Manager has now talked to Supervisor, who confirms that Employee did complain that one of her co-workers had submitted an inappropriate expense report. Supervisor felt the expense report was appropriate, and told Employee and all others in the group the same during a staff meeting. Supervisor also felt that Employee's retaliation complaint was nothing more than an attempt to deflect attention from her poor performance. Manager has now examined the expense report in question. From what he can determine, the supervisor and a number of his employees (including the complaining Employee) had gone out for a very expensive dinner, and Supervisor had "allowed" one of the subordinates to expense it so that Supervisor could then approve the expense report. Manager agrees with Employee that this process was inappropriate, but he is inclined to agree with Supervisor that Employee is a poor performer. Any new concerns?
- Coincidentally, Manager has received a call from another Company Manager regarding Employee. Apparently, Employee has applied for a position in another department and the other Manager is looking for a reference. What is your advice?

ACC's 2005 Annual Meeting: Workplace Privacy

October 17-19, Marriott Wardman Park Hotel



## Managing Private Medical Information

- HIPAA
  - Personal Health Information – *PHI*
  - Depends on source – Benefit Plan? Health care provider?
  - Most *stringent* duty to protect
- ADA/FMLA
  - Use generally limited to legitimate purpose of identifying need for and or reasonable accommodations or eligibility for leave.
  - Maintain apart from personnel file records, limited disclosure
- State Laws
  - E.g. California Medical Privacy Act
  - Workers Compensation Laws

ACC's 2005 Annual Meeting: Workplace Privacy

October 17-19, Marriott Wardman Park Hotel



## WHAT IF ... (Hypo No. 3)

- A supervisor in your client organization asks for your help in accommodating one of his analysts. The employee recently had a difficult pregnancy and spent the last 12 weeks of the pregnancy off work and in bed. While the birth went smoothly and the employee has a healthy child, she states she has no family to support her, and the spouse left town after draining her bank accounts. He has been periodically returning to town, however, and has been physically abusing the employee on those occasions. The supervisor knows the employee needs her job, but also knows she can only work about 15 hours a week because that's as much child-care as she can afford. He asks whether he can accommodate her with some combination of leave that will permit her to retain her full time job while working only 3 hours a day until she gets "back on her feet." What is your advice?

ACC's 2005 Annual Meeting: Workplace Privacy

October 17-19, Marriott Wardman Park Hotel



## WHAT IF ... (Hypo No. 4)

- Suppose the EE is off work due to a non-industrial illness rather than pregnancy. Supervisor wants to know Analyst's reasons for not being at work and when Analyst might return. Analyst tells supervisor that her doctor has her off work for two weeks at a time between appointments and that she is taking certain specific pain and anti-depressant medications. FMLA/Sick Leave administrator has a doctor's explanation that Analyst has been diagnosed with incapacitating physical and mental illness. What information can he receive from Plan Administrator? From FMLA administrator? What if EE discloses the diagnosis? What can Supervisor do or say?
- Supervisor has upgraded HotShot, into Analyst's job during absence. HotShot hounds Supervisor about permanent promotion. HotShot wants to transfer but Supervisor really needs Hot Shot to stick around for an immediate project deadline and long term projects in case Analyst doesn't come back. What information can he share with HotShot? With other workers?

ACC's 2005 Annual Meeting: Workplace Privacy

October 17-19, Marriott Wardman Park Hotel



## Drug/Alcohol & Other Testing

- Drug Free Workplace Acts
- Common Testing Issues
  - Applicant Testing
  - Particularized Suspicion (for cause)
  - Random Testing
  - Post-Accident
- Psychological Testing
- Privacy of results

ACC's 2005 Annual Meeting: Workplace Privacy

October 17-19, Marriott Wardman Park Hotel



## WHAT IF ... (Hypo No. 5)

- Your Company has a U.S. DOT random drug testing program for certain bargaining unit and other employees who operate company commercial vehicles. EE phones in 30 minutes before start time to request a *day off*. Supervisor says we're too busy, can't authorize, you need to come in. EE reports and is then told he has been selected for random testing. He reports to the site and requests a steward. The 3<sup>rd</sup> party sample collection representative tells EE that s/he still needs to give a sample. The EE gives a sample without further comment and returns to his regular duties. The next day EE comes to work and says, he doesn't think the results may be very good because he has been taking medication for pain. EE then resigns. Drug results come back positive for amphetamines.
- What can you do with the information? What about the steward request? What must you consider based on the employee's statements? What if the EE had said he has a drug/alcohol problem? Does when such information is revealed change the outcome?
- What if the employee doesn't give a sample claiming s/he can't? What if he reports the next day with a doctor's note asserting EE has 'shy bladder'?



## Personal Information from 3<sup>rd</sup> Parties

- Credit Histories
- Employment references, letters of recommendation
- Criminal Records, Info re Off Duty Misconduct
  - Driving records
  - Police reports



## WHAT IF ... (Hypo No. 6)

- You are paged out of an all-hands meeting by one of the newer managers in your client organization. When you call him, you hear panic in his voice.
- The manager reports to you that one of his subordinates, an *analyst* in a *small support organization* at a *regional office* was on the *11 o'clock news*. The news story was that the employee, who coaches soccer in his off-hours, was *arrested for unlawful sexual intercourse with a minor* after one of the girls on his soccer team told her parents that she was having an affair with him. The employee called in early this morning and left a message on the manager's voicemail indicating that he was going to be *out sick today*. The employee's *co-workers are all discussing* the news, and the manager says he feels he cannot have the employee return to work because it will be *too disruptive*. However, the *employee is critical* to the manager's operations, and so the manager asks if he can have him *work from home*. What advice?



## Global Issues Involving Workplace Privacy- Jim Beyer



## EU Directive on Data Protection

- Any information processed that identifies or could identify any person, and, thus, includes data concerning recruits, employees and former employees.
- [http://europa.eu.int/comm/justice\\_home/fsj/privacy/](http://europa.eu.int/comm/justice_home/fsj/privacy/)



## WORKPLACE PRIVACY POLICY

- **Contents**
- Definition of "Employee Information" (or "Personal Data", etc.)
- Identification of information subject to the Policy
- Statements regarding the organization's Employee Information management practices, including disclosures:
  - Internal and external
  - National and international
- Reasons for the collection, use and/or disclosure of the Employee Information
- Rights of access and correction of information held





## WORKPLACE PRIVACY POLICY.

- Nature of consent given, process for withdrawal and consequences
- Retention and destruction practices
- Security measures adopted in protecting information
- Acceptance/acknowledgement

ACC's 2005 Annual Meeting: Workplace Privacy

October 17-19, Marriott Wardman Park Hotel



## THE PROBLEM

- Competing standards in different jurisdictions
- Single standard approach requires adopting most onerous standards everywhere
- E.g.
  - E-mail/Internet Monitoring
    - Single standard would prohibit monitoring everywhere
    - May be human rights violation in some jurisdictions
    - May even be criminal violation

ACC's 2005 Annual Meeting: Workplace Privacy

October 17-19, Marriott Wardman Park Hotel



## THE SOLUTION

- **Hybrid Approach:**
- One standard wherever possible:
  - Consistency
  - Simpler
  - General corporate approach
- Differing national and regional standards where necessary and/or strategic



## Examples

- France's highest appellate court held in *Nikon France v. Onos*, that employers do not have the right to read their employees' personal electronic mail or other personal computer files. A French business terminated an engineer's employment after a search of his e-mail and word processing files revealed that he was performing unauthorized freelance work during business hours. As the relevant computer files were marked "personal," the engineer sued Nikon saying his rights to workplace privacy and secrecy of correspondence were violated. The high court agreed, holding that an employer cannot intercept an employee's e-mail, or read e-mail marked "personal," even if the company prohibits personal use of company computers.



**Examples:**

- Italy- the Italian Data Protection Commission decided that employees generally have the right to access any document containing their personal data in the possession of their employer. Italian privacy law grants individuals the right to access personal data collected about them. An employee accordingly requested from his former employer all e-mails containing his professional evaluations, and appealed to the DPA after the employer refused to disclose these materials. The DPA ruled that companies are required to extract from documents in their possession (other than personal communications) all personal information concerning the requesting employee and to communicate such information to the employee in an easily understandable form.

ACC's 2005 Annual Meeting: Workplace Privacy

October 17-19, Marriott Wardman Park Hotel

[Consulting](#)  
[Enterprise](#) [Services](#)  
[Solutions / ATS](#)

View Policies by...  
[Title](#)  
[Number](#)

[Policies->Legal](#)  
[Finland Supplement](#)  
[Data Privacy](#)

[NATURE OF REVISIONS](#) | [PURPOSE](#) | [SUPPLEMENT GUIDELINES](#) | [SUPPORTING DOCUMENTATION](#) | [CONTACT INFORMATION](#)

All policies/supplements are subject to local laws where the Company operates. These policies/supplements are subject to change without prior notification.

Applies to:	All employees in: Consulting, Enterprise, Services, Solutions / ATS
-------------	--

Supplement Number:	0090_C13	Effective Date of this Version:	25 March 2005
Associated Global Policy:	<a href="#">Policy 0090 - Data Privacy</a>	Supersedes the Version Dated:	2 June 2004
Policy Sponsor:	Legal and Commercial	Original Effective Date:	1 October 2001

NATURE OF REVISIONS FROM LAST VERSION

March 10, 2005 -- Added appropriate organizations for viewing policy.

[BACK TO TOP](#)

PURPOSE

The data privacy policy sets out the duties of Accenture and its employees when processing personal data about individuals and describes the rights of individuals in relation to their personal data processed by Accenture. This country supplement details the changes that should be made to the global policy to reflect this country's data privacy legislation.

[BACK TO TOP](#)

SUPPLEMENT GUIDELINES

*Below, the Data Privacy Policy 90 is shown in its entirety and with the variations that are required under the Finland's data privacy laws incorporated.*

Table of Contents

- [1. Scope and application of the policy](#)
- [2. Accenture's duties](#)
- [3. An individual's rights:](#)
  - [3.1 Right of access to personal data](#)
  - [3.2 Right to correct personal data](#)
  - [3.3 Right to object to direct marketing](#)
  - [3.4 Right to object to processing for compelling reasons](#)
  - [3.5 Rights in relation to automated decision taking](#)
- [4. Ensuring compliance of this policy](#)

**1. Scope and Application**

This policy regulates the way in which Accenture (the company) obtains, uses, holds, transfers and otherwise processes personal data about individuals and ensures all its employees understand the rules about protecting personal data. It also explains individuals' rights in relation to their personal data processed by the company. This policy does not apply to processing of personal data on behalf of clients of the company and other third parties.

This policy is a country specific supplement to the company's implemented global policy (90). This country supplement is designed to regulate the processing of personal data in accordance with Finland's specific laws. Country supplements, together with the global policy, ensure that all Accenture employees understand the company's obligation to abide by the data privacy laws and regulations of all of the countries in which the company operates.

Guidelines are available to help employees interpret and act in accordance with the global policy. The global guidelines are attached as a supporting document to the global policy. Employees should be aware, however, that localized versions of these guidelines exist for a number of countries where they have localized the global policy. It is advisable therefore to contact Finland's Data Privacy Officer to ascertain if localized guidelines apply in Finland.

The company may from time to time post pictures of individual employees on its website and use them in our advertisements. Such pictures could constitute personal data and therefore will be processed in accordance with this policy and Finland's personal data laws. For more information, please contact Christian Wikström.

Where the company controls other company entities (whether by virtue of contract, partnership, ownership of shares or otherwise), that other company will be required to abide by the principles set in this policy.

The company processes personal data about its employees, the employees of its clients and suppliers and any other individuals, including job applicants, former partners and former employees, for a number of business purposes, including:

Scheduling

Recruitment

Employee performance management and professional development

Payroll, fund management and accounting

Business and market development

Building and managing external relationships

Planning and delivery of business integration capabilities

Research and development

Technology infrastructure and support and facilities management

Travel management

Knowledge management

Other purposes required by law or regulation

See Supporting Documentation below for the definitions on "company" and "personal data".

[Back to Table of Contents](#)

## 2. The company's duties

To protect the personal data that comes into the company's possession, all company entities will observe the following policy guidelines:

(a) The company will process personal data fairly and lawfully. In particular, the company will not process personal data at all unless one of the following conditions is met:

(i) the individual concerned has consented to the processing;

(ii) the company needs to carry out the processing (1) to perform, or take steps at the request of an individual prior to entering into, a contract with the individual concerned (2) to comply with legal obligation or (3) to protect the vital interests of the individual concerned in a 'life or death' situation or;

(iii) there is a relevant connection between the individual and the operations of the company, based on the individual being a client or member of, or in the service of, the company;

(iv) processing is necessary for purposes of payment traffic, automated data processing or other comparable tasks undertaken on the assignment of another;

(v) the matter concerns generally available data on the status, duties or

performance of a person in a public corporation or business, and the data is processed in order to safeguard the rights and interests of the company or a third party receiving the data;

(vi) Finland's Data Protection Board has authorized the same; or

(vii) the company needs to carry out the processing to pursue the company's legitimate interests, and those interests are not overridden because the processing prejudices the interests or fundamental rights and freedoms of the individual concerned, and such processing has been authorized by Finland's Data Protection Board.

(b) When an individual gives the company personal data about him or herself, the company will make sure that the individual knows who they are and what they intend to do with the data provided. The company will also observe procedures designed so that individuals giving the company their personal data are provided with any additional information that may be necessary so that the processing of the data is fair.

(c) Where collecting personal data about an individual indirectly (for example, from a published source), the company will inform the individual that the company will collect the data and what the company intends to do with the data. In addition, where such individual is a job applicant or an employee of the company, the company will on a case-by-case basis obtain a consent from the individual before collecting any personal data about the individual indirectly. The company will not obtain such consent, when an authority discloses data to the company for the company's purpose of carrying out its legal obligations, or when the company obtains credit information or criminal records to determine the reliability of an employee or a job applicant.

The company will also observe procedures designed so that the individual is provided with any additional information that may be necessary so that the processing of the data is fair, unless the effort involved would be disproportionate to the value to the individual of being informed.

(d) The company does not generally seek to collect data relating to the following:

Racial or ethnic origin

Political opinions

Religious or other similar beliefs

Trade union membership

Physical or mental health

Sexual life

Criminal record.

The company will not collect such data at all unless i) the individual concerned agrees in writing that the company may do so, on the basis of a full understanding of why the company is collecting the data or ii) where the company needs to do so to meet its obligations or exercise its rights under employment law or iii) in exceptional circumstances such as where the processing is necessary to protect the vital interests of the individual concerned.

The company may in some exceptional circumstances rely on consent given on behalf of the individual, for example by a company employee on behalf of a family member.

(e) The company will have procedures and systems to ensure that:

(i) it does not collect excessive personal data; and

(ii) the personal data it holds are adequate (given the purposes for which they are collected), relevant to those purposes, accurate, up to date; and

(iii) it processes personal data only for the purposes specified in this policy or in information given to the individual concerned; and

(iv) the personal data of company's employees or job applicants is directly necessary for their employment relationship.

(f) The company will observe retention policies and procedures designed so that it deletes personal data after a reasonable time, given the purposes for which the personal data is held, except where, given those purposes, it is necessary to keep the personal data indefinitely, or another law requires the data to be kept for a certain time. When the company no longer needs to keep

personal data for the purposes for which they are held it will destroy them as soon as practicable.

(g) The company will have in place organizational, physical and technical security arrangements in relation to all of the personal data that it holds. It will ensure those arrangements are appropriate to the risks represented by the processing it carries out of those personal data and the nature of those personal data. Where appropriate, these arrangements will include arrangements for 'need to know' access to personal data.

The company recognizes, in particular, that adequate security is important where it arranges for outside service providers to process personal data on its behalf. Where the company establishes such arrangements they will ensure that the service providers are bound by written contracts under which they agree to act only on the company's instructions and to have appropriate security arrangements in place to protect the personal data.

(h) The company recognizes that personal data needs to be treated with care in countries which do not have data protection laws, or whose data protection laws do not provide as high a level of protection as has become the accepted standard in the European Union. In those countries the company will not transfer personal data to third parties for further processing (other than merely for processing on the company's behalf) unless they make a binding contractual commitment to abide by a data privacy standard at least as high as this policy in relation to the data. The only exceptions are where:

(i) the transfer is necessary 1) to protect the vital interests of the individual concerned in a 'life or death' situation, or 2) to enter into or perform a contract with (or for the benefit of) that individual; or

(ii) that individual has consented to the transfer.

[Back to Table of Contents](#)

**3. An individual's rights**

**3.1 Right of access**

(a) On written request by an individual, and where the company have or are given sufficient information to allow the company to identify the individual making the request and decide whether it holds personal data about him or her, the company will:

(i) Inform that individual whether the company holds personal data about him or her;

(ii) Describe the data it holds, the reason for holding the data and the categories of person to whom it may disclose the data; and

(iii) Provide the individual with copies of the personal data held about him or her, together with an indication of the source(s) of the data.

(a) The company will provide this information and these copies within a reasonable period after the individual's request.

c) The company may, however, refuse to provide an individual with information in accordance with Finnish law, for instance, where disclosure of that information would jeopardize the rights of others (in which case the company will provide as much of the information as possible without revealing the information that might jeopardize the rights of others), unless the other agrees that the company may release the information.

**3.2 Right of correction**

(a) Individuals may request that the company corrects the personal data it holds about them. If the company agrees that the data are incorrect, it will delete or correct the data. If it does not agree that the data are incorrect, it will, nevertheless, record in the relevant file(s) the fact that the individual considers the data to be incorrect.

**3.3 Right to object to direct marketing**

(a) The company will abide by any request from an individual not to use his or her personal data for direct marketing purposes.

**3.4 Right to object to processing for compelling reasons**

(a) Where the company relies on the 'balance of interests' condition in paragraph 2 (a)(vii) above to justify the processing of personal data, the company will abide by any justified request from an individual to stop that processing of his or her data if the individual objects to the processing on

compelling and legitimate grounds.

**3.5 Rights in relation to automated decision taking**

(a) The company will not generally take decisions that significantly affect an individual solely on the basis of automatic processing of data that evaluates personal aspects of the individual (such as his or her performance at work, creditworthiness, reliability or conduct). Where the company does use such decision-making techniques it will observe procedures providing adequate safeguards to protect the legitimate interests of the individual.

[Back to Table of Contents](#)

**4. Ensuring compliance with this policy**

(a) Accenture has internal arrangements in place to ensure compliance with this policy, to allow effective exercise of individuals' rights guaranteed in the policy and to deal with any complaints from individuals that the company may not have complied with the policy. All individuals can call upon these arrangements and/or exercise their rights by contacting their local Data Privacy Officer.

[Back to Table of Contents](#)

[BACK TO TOP](#)

SUPPORTING DOCUMENTATION

**Definitions:**

'company'
Accenture Ltd. (an exempted company registered in Bermuda under Number EC 30090) and any Accenture Affiliate, which together comprise the Accenture Group. "Accenture Affiliate" shall mean any entity, whether incorporated or not, that is controlled by or under common control with Accenture Ltd. and subscribes generally to the policies and procedures of the Accenture Group, and "control" (or variants of it) shall mean the ability whether directly or indirectly to direct the affairs of another by means of ownership, contract or otherwise

'personal data'
Information about living individuals which is held in automatically processable form (for example, on a computer) or in a structured manual filing system.

[BACK TO TOP](#)

CONTACT INFORMATION

Questions and requests related to this policy in Finland and Nordic can be sent to Data Privacy contact, Kaisa Eskelin, [kaisa.eskelin@accenture.com](mailto:kaisa.eskelin@accenture.com) tel. +358 205725 546. For global data privacy matters or any other data privacy query, contact [hojana.bellamy@accenture.com](mailto:hojana.bellamy@accenture.com), Octel 43-46879.

[BACK TO TOP](#)

**Related Terminology:**

Copyright 2001-2005 Accenture. All Rights Reserved. Accenture Confidential. For Internal Use Only. [Terms of Use/Privacy Statement](#)

[Home](#)
[About](#)
[Contact](#)
[Help](#)
[Advanced Search](#)

[Consulting](#)  
[Enterprise Services](#)  
[Solutions / ATS](#)

Policies > Legal  
 Global Policy  
 Data Privacy

View Policies by...  
[Title](#)  
[Number](#)

[NATURE OF REVISIONS](#) | 
 [PURPOSE](#) | 
 [POLICY](#) | 
 [SUPPORTING DOCUMENTATION](#) | 
 [SUPPLEMENT\(S\)](#) | 
 [CONTACT INFORMATION](#) | 
 [BACKGROUND/RATIONALE](#)

All policies/supplements are subject to local laws where the Company operates. These policies/supplements are subject to change without prior notification.

Applies to:	All employees in: Consulting, Enterprise, Services, Solutions / ATS
-------------	--

Policy Number:	0090	Effective Date of this Version:	18 July 2005
Policy Sponsor:	Legal and Commercial	Supersedes the Version Dated:	24 March 2005
		Original Effective Date:	1 October 2001

**NATURE OF REVISIONS FROM LAST VERSION**

July 15, 2005 -- Removed outdated contact list from Supporting Documentation

March 16, 2005 -- Added appropriate organizations for viewing policy. Added link to Policy 0057 and removed link to Policy 0102 in the Supporting Documentation section; Policy 0102 has been incorporated into Policy 0057

[BACK TO TOP](#)

**PURPOSE**

The purpose of this policy is to set out the duties of Accenture and its employees when processing personal data about individuals and describes the rights of individuals in relation to their personal data processed by Accenture.

[BACK TO TOP](#)

**POLICY**

To facilitate the understanding of this policy, it is organized as follows:

- [1. Scope and application of the policy](#)
- [2. Accenture's duties](#)
- [3. An individual's rights:](#)
  - [3.1 Right of access to personal data](#)
  - [3.2 Right to correct personal data](#)
  - [3.3 Right to object to direct marketing](#)
  - [3.4 Right to object to processing for compelling reasons](#)
  - [3.5 Rights in relation to automated decision taking](#)
- [4. How Accenture ensures compliance with this policy](#)
- [5. When one Accenture entity processes personal data on behalf of another Accenture entity](#)

**1. Scope and Application**

This policy regulates the way in which Accenture (the company) obtains, uses, holds, transfers and otherwise processes personal data about individuals and ensures all its employees understand the rules about protecting personal data. It also explains individuals' rights in relation to their personal data processed by the company. In addition,

the policy regulates the circumstances in which one Accenture entity processes personal data on behalf of another Accenture entity. This policy does not apply to processing of personal data on behalf of clients of the company and other third parties.

The company also abides by localized variances to this policy. Such variances are designed to regulate the processing of personal data in accordance with a country's specific local laws, where they exist. These localized variances, together with this policy, ensure that all Accenture employees understand the company's obligation to abide by the data privacy laws and regulations of all of the countries in which the company operates. The localized variances are available as country supplements to this policy.

Guidelines are available to help employees interpret and act in accordance with this policy. The internal global guidelines are provided in the [Supporting Documentation](#) section below. Employees should be aware, however, that localized versions of these guidelines exist for a number of countries, where they have localized the global policy. It is advisable therefore to contact the country's local Data Privacy Officer to ascertain if localized policies and therefore localized guidelines apply.

Where the company controls other company entities (whether by virtue of contract, partnership, ownership of shares or otherwise), that other company will be required to abide by the principles set in this policy.

The company processes personal data about its employees, the employees of its clients and suppliers and any other individuals, including job applicants, former partners and former employees, for a number of business purposes, including:

- Scheduling
- Recruitment
- Employee performance management and professional development
- Payroll, fund management and accounting
- Business and market development
- Building and managing external relationships
- Planning and delivery of business integration capabilities
- Research and development
- Technology infrastructure and support and facilities management
- Travel management
- Knowledge management
- Other purposes required by law or regulation

[Back to Table of Contents](#)

**2. The company's duties**

To protect the personal data that comes into the company's possession, all company entities will observe the following policy guidelines:

- (a) The company will process personal data fairly and lawfully. In particular, the company will not process personal data at all unless one of the following conditions is met:
  - (i) the individual concerned has consented to the processing;
  - (ii) the company needs to carry out the processing (1) to perform, or take steps with view to entering into, a contract with the individual concerned (2) to comply with legal obligation or (3) to protect the vital interests of the individual concerned in a 'life or death' situation; or
  - (iii) the company needs to carry out the processing to pursue the company's legitimate interests, and those interests are not overridden because the processing prejudices the interests or fundamental rights and freedoms of the individual concerned.
- (b) When an individual gives the company personal data about him or herself, the company will make sure that the individual knows who they are and what they intend to do with the data provided. The company will also observe procedures designed so that individuals giving the company their personal data are provided with any additional information that may be necessary so that the processing of the data is fair.
- (c) Where collecting personal data about an individual indirectly (for example, from a published source), the company will inform the individual that the company holds the data and what the company intends to do with the

data. The company will also observe procedures designed so that the individual is provided with any additional information that may be necessary so that the processing of the data is fair.

This information will not be provided where the effort involved would be disproportionate to the value to the individual of being informed.

(d) The company does not generally seek to collect data relating to the following:

Racial or ethnic origin

Political opinions

Religious or other similar beliefs

Trade union membership

Physical or mental health

Sexual life

Criminal record.

The company will not collect such data at all unless: (i) the individual concerned agrees in writing that the company may do so, on the basis of a full understanding of why the company is collecting the data, or ii) the company needs to do so to meet its obligations or exercise its rights under employment law, or iii) in exceptional circumstances such as where the processing is necessary to protect the vital interests of the individual concerned.

The company may in some exceptional circumstances rely on consent given on behalf of the individual, for example by a company employee on behalf of a family member.

(e) The company will have procedures and systems to ensure that:

(i) it does not collect excessive personal data; and

(ii) the personal data it holds are adequate (given the purposes for which they are collected), relevant to those purposes, accurate, up to date and

(iii) it processes personal data only for the purposes specified in this policy or in information given to the individual concerned.

(f) The company will observe retention policies and procedures designed so that it deletes personal data after a reasonable time, given the purposes for which the personal data are held, except where, given those purposes, it is necessary to keep the personal data indefinitely, or another law requires the data to be kept for a certain time. When the company no longer needs to keep personal data for the purposes for which they are held it will destroy them as soon as practicable.

(g) The company will have in place organizational, physical and technical security arrangements in relation to all of the personal data that it holds. It will ensure those arrangements are appropriate to the risks represented by the processing it carries out of those personal data and the nature of those personal data. Where appropriate, these arrangements will include arrangements for 'need to know' access to personal data.

The company recognizes, in particular, that adequate security is important where it arranges for outside service providers to process personal data on its behalf. Where the company establishes such arrangements they will ensure that the service providers are bound by written contracts under which they agree to act only on the company's instructions and to have appropriate security arrangements in place to protect the personal data.

(h) The company recognizes that personal data needs to be treated with care in countries which do not have data protection laws, or whose data protection laws do not provide as high a level of protection as has become the accepted standard in the European Union. In those countries the company will not transfer personal data to third parties for further processing (other than merely for processing on the company's behalf) unless they make a binding contractual commitment to abide by a data privacy standard at least as high as this policy in relation to the data. The only exceptions are where:

(i) the transfer is necessary 1) to protect the vital interests of the individual concerned in a 'life or death' situation, or 2) to enter into or perform a contract with (or for the benefit of) that individual; or

(ii) that individual has consented to the transfer.

[Back to Table of Contents](#)

### 3. An individual's rights

#### 3.1 Right of access

(a) On written request by an individual, and where the company have or are given sufficient information to allow the company to identify the individual making the request and decide whether the company holds personal data about him or her, the company will:

(i) Inform that individual whether the company holds personal data about him or her;

(ii) Describe the data it holds, the reason for holding the data and the categories of person to whom it may disclose the data; and

(iii) Provide the individual with copies of the personal data held about him or her, together with an indication of the source(s) of the data

(b) The company will provide this information and these copies within a reasonable period after the individual's request, or within any specific period that may be required by local law in any country.

(c) The company may, however, refuse to provide an individual with information where disclosure of that information would reveal information about another individual (in which case the company will provide much of the information as possible without revealing information about the other individual), unless the other individual agrees that the company may release the information or the company decides that it is reasonable to provide the information without the other individual's agreement.

In addition, in some countries localized policies may provide for other legitimate reasons for refusing an individual's request for access, in accordance with national data protection law.

#### 3.2 Right of correction

(a) Individuals may request that the company corrects the personal data it holds about them. If the company agrees that the data are incorrect, it will delete or correct the data. If it does not agree that the data are incorrect, it will, nevertheless, record in the relevant file(s) the fact that the individual considers the data to be incorrect.

#### 3.3 Right to object to direct marketing

(a) The company will abide by any request from an individual not to use his or her personal data for direct marketing purposes.

#### 3.4 Right to object to processing for compelling reasons

(a) Where the company relies on the 'balance of interests' condition in paragraph 2 (a)(iii) above to justify the processing of personal data, the company will abide by any justified request from an individual to stop that processing of his or her data if the individual objects to the processing on compelling and legitimate grounds.

#### 3.5 Rights in relation to automated decision taking

(a) The company will not generally take decisions that significantly affect an individual solely on the basis of automatic processing of data that evaluates personal aspects of the individual (such as his or her performance at work, creditworthiness, reliability or conduct). Where the company does use such decision-making techniques it will observe procedures providing adequate safeguards to protect the legitimate interests of the individual.

[Back to Table of Contents](#)

### 4. Ensuring compliance with this policy

(a) Accenture has internal arrangements in place to ensure compliance with this policy, to allow effective exercise of individuals' rights guaranteed in the policy and to deal with any complaints from individuals that the company may not have complied with the policy. All individuals can call upon these arrangements and/or exercise their rights by contacting their local Data Privacy Officer.

### 5. When one Accenture entity processes personal data on behalf of another Accenture entity

Where a company entity processes personal data (the "Processed Data") on behalf of another company entity, the first such entity is referred to in this policy as the "Processor" and the second as the "Controller".


(a) The Processor will:

- (i) process the Processed Data only on the written instructions of the Controller;
  - (ii) implement appropriate technical and organizational measures to protect the Processed Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing;
  - (iii) process the Processed Data fairly and lawfully;
  - (iv) make all reasonable efforts to maintain the Processed Data so that they are accurate and up to date at all times;
  - (v) make all reasonable efforts to delete the Processed Data after a reasonable time, given the purposes for which they are held, unless it is appropriate to keep them indefinitely;
  - (vi) not disclose the Processed Data to any person except as required or permitted by any agreement between the Controller and the Processor or with the Controller's written consent;
  - (vii) provide full cooperation and assistance to the Controller in allowing the individuals to whom the data relate to:
    1. have access to those data; or
    2. require that those data are deleted or corrected if they are incorrect (or, if the Controller does not agree that they are incorrect, to require the fact that the individual considers the data to be incorrect to be recorded); and
  - (viii) not process the Processed Data except to the extent reasonably necessary to the performance of any agreement between the Controller and the Processor in relation to the Processed Data.
- (b) Section 5 of this policy (**when one Accenture entity processes personal data on behalf of another Accenture entity**) constitutes a written instruction from the Controller to the Processor, subject to paragraph (a), to take such steps in the processing of the Processed Data as:
- (i) the Processor reasonably considers necessary or desirable for the performance of any agreement between the Controller and the Processor in relation to the Processed Data; and
  - (ii) Are consistent with the Processor's obligations under any such agreement and any other applicable laws and regulations.

[Back to Table of Contents](#)

[BACK TO TOP](#)

SUPPORTING DOCUMENTATION

Frequently Asked Questions 

Refer also to the following policies:

- [Confidentiality - Policy 0069](#)
- [Meritocracy - Policy 0078](#)
- [Intellectual Property - Policy 0091](#)
- [Security of Information and Acceptable Use of Systems - Policy 0057](#)
- [Security - Policy 0785](#)

**Internal Global Guidelines** These guidelines provide an interpretation of the global data privacy policy and serve as a reference for internal use, when Accenture employees are called up to explain the policy and answer questions for other Accenture employees. The global guidelines are currently under review but are available from Accenture's Global Data Privacy Compliance Lead, Bojana Bellamy.

The global guidelines address four main groups for which data privacy principles apply: Accenture employees and potential recruits, client employees and other representatives, suppliers' employees and other individual contacts and Accenture web sites.

The global guidelines will also be reviewed by local counsel and localized as necessary to meet legal requirements of specific jurisdictions. Therefore, please check with the local

Data Privacy Officer or L&C Lead for Data Privacy to see if localized guidelines apply.

**Internal Global Templates** In addition to the data privacy policy, standard wording templates were developed for Accenture employees to use when creating contracts or obtaining consent for data processing and in various other circumstances. The templates can be obtained from the local Data Privacy Officer or the local L&C Lead for Data Privacy. The templates have also been reviewed by local counsel and localized as necessary to meet legal requirements of specific jurisdictions.

**Definitions**

'company' - Accenture Ltd. (an exempted company registered in Bermuda under Number EC 30090) and any Accenture Affiliate, which together comprise the Accenture Group. "Accenture Affiliate" shall mean any entity, whether incorporated or not, that is controlled by or under common control with Accenture Ltd. and subscribes generally to the policies and procedures of the Accenture Group, and "control" (or variants of it) shall mean the ability whether directly or indirectly to direct the affairs of another by means of ownership, contract or otherwise

'personal data' - Information about living individuals which is held in automatically processable form (for example, on a computer) or in a structured manual filing system.

[BACK TO TOP](#)

SUPPLEMENT(S)

The county supplements attached to this section of the policy provide the variances to the global policy necessitated by additional requirements of local data protection/privacy laws. If necessary, the country supplement has been translated into the local language.

Country supplements should exist for many of the regulated countries; however, they are not yet available in all cases. They will be added as they become available. In the meantime, please contact the local data privacy officer (see 'Contacts'), to discuss if localization applies.

Country supplements are currently in progress for France, Austria, Luxembourg, Denmark, Germany, Ireland, Poland and Switzerland.

Country supplements available now and linked here:

Country - Language
<a href="#">Australia - English</a>
<a href="#">Belgium - English</a>
<a href="#">Canada - English</a>
<a href="#">Finland - English</a>
<a href="#">Hong Kong - English</a>
<a href="#">Hungary - English</a>
<a href="#">Hungary - Hungarian</a>
<a href="#">Italy - English</a>
<a href="#">Japan - English</a>
<a href="#">(The) Netherlands - English</a>
<a href="#">(The) Netherlands - Dutch</a>
<a href="#">Norway - English</a>
<a href="#">Poland - English</a>
<a href="#">Russia - English</a>
<a href="#">Russia - Russian</a>
<a href="#">Spain - English</a>
<a href="#">Spain - Spanish</a>
<a href="#">Sweden - English</a>
<a href="#">United Kingdom - English</a>

[BACK TO TOP](#)

CONTACT INFORMATION

Questions related to this policy can be sent to the appropriate country Data Privacy Officer. Refer to the list of country Data Privacy Officers. For global data privacy matters or any other data privacy query, please contact [bojana.bellamy@accenture.com](mailto:bojana.bellamy@accenture.com), who is Accenture's Global Data Privacy Compliance Lead, Octel 43-46879

[BACK TO TOP](#)

BACKGROUND/RATIONALE



[BACK TO TOP](#)

---

**Related Terminology:** data protection

Copyright 2001-2005 Accenture. All Rights Reserved. Accenture Confidential. For Internal Use Only.  
[Terms of Use/Privacy Statement](#)

## Data Privacy in Accenture

### Frequently Asked Questions (for [Policy 90](#))

#### What are personal data?

Personal data is any information about a particular individual that is stored either electronically or in a manual filing system. This includes information about our employees, job applicants and clients. Even though Accenture's clients are corporations or other legal entities, the company interacts with individual client employees and other representatives. In some jurisdictions, personal data also includes corporate data.

Personal data stored by Accenture includes such items as: names and contact details to support the purchasing, payment, billing and collection activities of Accenture; name and contact information, details of contacts with individuals (e.g., past meetings) to support Accenture in client selection and development, as well as in opportunity assessment and selling.

Personal data can be as little as name and contact details, and as much as opinions, appraisals, and intentions in relation to particular individuals.

#### What are sensitive personal data?

Some categories of personal data are defined by national data protection/privacy laws as sensitive personal data. The types of sensitive data can vary by country, but generally include: racial or ethnic origin, political opinions, religious or other similar beliefs, trade union membership, physical or mental health, sexual life, or criminal record.

Sensitive data is subject to stricter legal requirements and is only collected by Accenture in limited circumstances to support specific business purposes. In fact, in most countries, we do not collect sensitive personal data in many of the categories listed above. As a rule, we will collect and process sensitive personal data only when the individual concerned agrees in writing and understands why we are collecting it. Examples:

In some countries, we may hold limited information on client dietary and smoking/non-smoking requirements for events and conferences, which could indicate religious, or other beliefs, ethnic origins, or health status.

In some countries, we may hold limited information on client likes/dislikes (e.g., interest in a particular association, such as Boy Scouts, etc.) to support Accenture in client selection and development, as well as in opportunity assessment and selling.

#### What does the data privacy policy 90 provide?

The policy provides a globally and consistent standard to govern the collection, handling, storage, transfers and security of personal data that Accenture holds, either directly or indirectly, about individuals (partners, employees, job applicants, clients, vendors, or any other individual).

The policy states that such information will only be collected and retained as necessary to support ongoing business operations. Furthermore, the policy outlines that the data should be protected, maintained and deleted when no longer needed. The policy also provides for rights of individuals, such as a right to request a copy of information that is held about them.

Do we share data across country borders?

Yes. Certain data transfers need to occur because of Accenture's global systems and global processes. Often, data from multiple countries is consolidated onto one server. Or, data from many countries is sent to one service center for processing, such as accounts payable.

It is because of the global nature of Accenture and the increasing number of national data protection/privacy laws throughout the world that we needed to formally establish and follow global data privacy procedures to enable Accenture to transfer data freely between all the countries in which we operate. Before this policy was in place, it was becoming increasingly difficult to transfer some data across borders and this was adversely affecting Accenture's business operations. The only way in which we can ensure unhindered internal data flows across borders is to comply with our data privacy policy throughout the world, even in countries without data protection/privacy laws.

How does this policy impact engagement and project teams?

Engagement/project teams need to understand the Data Privacy Policy and follow it in their interactions with client and vendor personnel. For example, if they collect personal data, they need to tell people why data is being collected (if the purpose is not obvious), what will be done with it, who will have access to it and why.

They should not collect personal data, especially sensitive data, unless there is a specific business reason to do so. If they collect data and later determine it is not needed, then that data should be destroyed. (Example: If they collect demographic information about client employees through power maps and find that they do not need some of the data for their analysis, they should destroy the excess data.)

These policies and processes refer to personal data that is stored or processed on systems that belong to Accenture. If they are processing data on behalf of a client (for example, in a Business Process Management engagement), they should continue to follow the client's instructions and not seek to impose Accenture's internal procedures on the client. Our clients need to decide the best approach for their particular circumstances regarding data privacy compliance.

The Data Privacy Policy does not apply to processing of personal data on behalf of clients of Accenture and other third parties. If you need assistance, please contact your local data privacy officer, see 'contacts'.

What effect does the policy have on client and other third party agreements?

The standard client and supplier agreements should include language (section L of the Templates that are available from the local data privacy officer) explaining that Accenture may collect some personal data information from client or vendor personnel, either directly or indirectly, and that the information may be used and disclosed for purposes connected with that particular agreement and for the relevant purposes specified in the Data Privacy Policy. You should make sure that this wording is in all new agreements and contract renewals, whether for a new or an existing client or vendor. However, you do not have to change current contracts.

If we put in place arrangements under which a third party (such as a marketing, or a credit card company, conference organizer, any service provider) processes personal data on behalf of Accenture, you should make sure that the arrangement is governed by a written contract including a provision based on Section Q of the Templates. This provision requires the vendor to process Accenture's personal data only on the firm's instructions and to have appropriate security arrangements. (This requirement does not apply to arrangements within Accenture, such as the outsourcing of data processing from Accenture in France to the European Service Center in Dublin. Such arrangements are covered by section 5 of the Data Privacy Policy). Note, it will often be necessary to include wording from both Templates L and Q in the same document, since Accenture will often process personal data about supplier employees and representatives when those suppliers are contracted to process personal data on behalf of the firm.

Business Process Management arrangements are currently outside the scope of the data privacy program. Separate guidelines and template contract language may be rolled out in the future. If you need assistance, please contact your local data privacy officer.

Can I see the data Accenture holds on me?

Yes, you can. This is known as a subject access request. The request must be made in writing to the local Data Privacy Officer (see contacts). Accenture has a duty to respond within a reasonable period, or any specific period provided by the national data protection/privacy law.

We may refuse to give access to some data, where giving information would reveal information about another individual and breach their privacy and our duty of confidentiality, unless that other individual has given his/her consent for such disclosure. Also, local data protection legislation in countries where we operate may provide for additional limited circumstances in which we may withhold information from the subject access request. Where applicable, these are described in localized policies for some countries. .

Can I get the information Accenture holds corrected?

Individuals may request that the company corrects the personal data it holds about them. The company will delete or correct any inaccurate data. . Where the company does not agree with the individual the company will, nevertheless, record in the relevant file(s) the fact that the individual considers the data to be incorrect.

What will happen if Accenture or its employees fail to comply with this policy?

In countries with data protection/privacy legislation, consequences may be severe:

Firstly, national data privacy authorities have considerable enforcement powers, such as to prohibit flows of data to a country which does not provide an adequate level of protection for personal data, ask Accenture to stop particular processing of personal data and delete a database.

Specific breaches of national data protection/privacy law, such as unauthorised disclosure of personal data, are criminal offences for which both Accenture and/or individual employees at all levels may be prosecuted.

Individuals can claim compensation through national courts for damage and distress resulting from any breach of national data protection/privacy legislation by Accenture, or our agents and service providers acting on our behalf. Individuals can also complain to the national data privacy supervisory authorities, which may lead to investigation, audits and enforcement.

Finally, in all countries, Accenture may face adverse publicity for as a result of a privacy related investigation, claim or enforcement. Privacy advocates and watchdogs, particularly in the USA, have been very prominent in brining attention to alleged data privacy violations by multinational corporations.

It is important that all Accenture entities world-wide and all Accenture employees observe this Data Privacy Policy to ensure we minimise the risk of adverse action from national data privacy supervisory authorities, individuals and privacy watchdogs.

Where do I go to get more information?

If you have a specific question that is not answered in the 'frequently asked questions', please contact your local data privacy officer. See Contacts.

Bojana Bellamy is Accenture's, Global Compliance Lead for Data Privacy. She is available to address any questions relating to data privacy, whether on a geographic or a functional basis.

[Consulting](#)  
[Enterprise](#) [Services](#)  
[Solutions / ATS](#)

View Policies by...  
[Title](#)  
[Number](#)

[Home](#)[About](#) | [Contact](#)[Help](#)[Advanced Search](#)

Policies>CIO/Information Technology  
Global Policy  
Security of Information and Acceptable Use of Systems

[NATURE OF REVISIONS](#) | [PURPOSE](#) | [POLICY](#) | [SUPPORTING DOCUMENTATION](#) | [SUPPLEMENTS](#) | [CONTACT INFORMATION](#) | [BACKGROUND/RATIONALE](#)

All policies/supplements are subject to local laws where the Company operates. These policies/supplements are subject to change without prior notification.

Applies to:	All employees in: Consulting, Enterprise, Services, Solutions / ATS
-------------	--

Policy Number:	0057	Effective Date of this Version:	8 July 2005
Policy Sponsor:	CIO	Supersedes the Version Dated:	23 March 2005
		Original Effective Date:	25 July 1997

**NATURE OF REVISIONS FROM LAST VERSION**

March 8, 2005 - Completely new sections include: acceptable use of client e-mail and rebooting Company computers to obtain security patches. Several sections were added/updated to include information from Policy 0102 and a few changes were made to the sections: Using IM Messages securely and Acceptable use of Non Company owned machines. Title change, incorporation of content from Policy 0102.

March 18, 2005 - Added 2 sentences to section 7.1 Acceptable Use of Accenture E-mail. Updated applies to information and organization-specific information.

March 23, 2005 - Updated metadata; no content updates.

July 7, 2005 - Modified Section 2.0 to include the word "personal" in order to make this more clear.

[BACK TO TOP](#)

**PURPOSE**

The purpose of this policy is to provide a comprehensive set of security requirements to ensure protection of confidential Company, client, and third party information entrusted to the Company or to which access is otherwise available. As Company users frequently need access to Company systems and the Internet to conduct business, this policy provides acceptable use requirements when working on a Company system.

[BACK TO TOP](#)

**POLICY**

**NOTICE OF COMPLIANCE**

Security is the responsibility of everyone affiliated with the Company, or directly accessing Company systems, Company data, and data entrusted to the Company by our clients or other third parties. The security measures described herein define the basic minimum level of security required for Company systems and information. Non-compliance with the required security measures and behaviors outlined in this policy could pose significant business and legal risk to the Company, and may create a potential for legal actions that could significantly impact the Company's operations and damage its business assets and reputation. Therefore, compliance with this policy and all Company security-related policies, are mandatory conditions for employment for all Company people, as well as any third parties (such as outsourcing providers, contractors, alliance partners, clients, etc.) that access Company systems or data. No one is permitted to bypass the security mechanisms provided by Company systems or infrastructure for any reason. Failure to comply with this policy will be reported and disciplinary action may be taken. Such action may include, but is not limited to, reprimand, financial penalties, termination of employment, and/or legal action.

The following are additional resources that will assist users with compliance or general questions:

- [Examples and Frequently Asked Questions](#), provides answers to common questions
- [Supporting Documentation](#), provides links to Procedures, Standards, Guidelines, and other Policies that are in support of this Policy
- [Contact](#), provides email addresses and/or phone numbers for people that can be contacted for additional assistance.

*Note: The Company's policies mandate what must be done and standards tell you how to be compliant with policy.*

**Exceptions, Migration, and Timeframes**

All people and all Company systems must comply with the statements in this policy immediately. Where a longer transition is required to achieve compliance, a documented business justification must be submitted with proposed timelines to the [Security Exceptions site](#) for approval.

Any exceptions to this Policy must be clearly documented and submitted to the [Security Exceptions site](#) for evaluation and approved. Only exceptions which have been approved are valid.

**TABLE OF CONTENTS**

[Security of Information and Acceptable Use of Systems](#)

[Purpose](#)

[Policy](#)

**NOTICE OF COMPLIANCE**

[Exceptions, Migration, and Timeframes](#)

[1.0 Scope](#)

[2.0 Overview](#)

[3.0 User IDs and Authentication](#)

[4.0 Access Rights](#)

[5.0 Privacy](#)

[6.0 Confidentiality](#)

[7.0 Required Security Behaviors for Acceptable Use](#)

[8.0 Communication of Trade Secrets](#)

[9.0 Disclaimer of Liability for Use of the Internet](#)

[10.0 Physical Security](#)

[Examples and Frequently Asked Questions](#)

[Supporting documentation](#)

[Country Supplement\(s\)](#)

[Contact](#)

[General Policy Questions](#)

[Technology Questions or Assistance](#)

[Computer Incident Response Team \(CIRT\)](#)

[Legal Questions](#)

[Security Exceptions Website](#)

**1.0 Scope**

**1.1 Users**

The following users are in the scope of this Policy:

- All Company people
- All third-party personnel requiring access to Company systems. This includes contractors, off-site providers of Company systems, employees and contractors of Company affiliated

companies, and professional service providers such as lawyers, auditors, accountants, and consultants.

- Company people and third parties accessing non-Company e-mail or resources, but identifying themselves as [affiliated with the Company](#)
- Company people and third parties accessing the Internet via a Company-owned computer or a non-Company owned computer connected to the Company network
- Company people and Company-hired contractors accessing client resources

The following users are out of scope of this Policy:

- Any personnel that do not require access to Company applications or technology infrastructure resources
- Public individuals accessing the Company's Internet websites (e.g., <https://publishing.accenture.com/Policies/CIOTechnology/www.accenture.com>)
- Company client personnel and their contractors accessing designated Company engagement sites

**1.2 Systems**

The systems in scope for this policy include all computers, data center resources, communications devices, and facilities that house Company information or provide access to Company data and systems for in-scope users.

[Back to TOC](#)

**2.0 Overview**

Company resources, including servers, e-mail and Internet access, applications, as well as laptops and workstations distributed to employees and contractors, are intended for official Company business use. Limited, personal use is also acceptable. Please reference the [Acceptable Use Standard](#) for examples of activities considered misuses of Company resources.

**3.0 User IDs and Authentication**

**3.1 User IDs**

**3.1.1 Protection**

Users must not share their user ID/password with anyone (e.g., executives must not share their user IDs with their Executive Assistants). An exception to this is that users may provide their passwords at their discretion to authorized Company technical support personnel, only if the user has initiated a maintenance request. At the completion of the maintenance, the user must change their password. Tokens and their associated PINs may not be shared at any time. Additional required steps for protecting passwords and tokens PINs are outlined in the [Identification and Authentication standard](#). Each user is responsible for all actions taken on the system with their user ID, and will be held accountable for both permitted and potentially unauthorized use of the system. Users must never use someone's ID, with the exception of Company technical support when required to provide maintenance on the user's computer. Any security related concerns must be reported immediately to [CIO Technology Services or the local technology support provider](#), and/or to the [Computer Incident Response Team \(CIRT\)](#), in accordance with the [Security Incident Handling](#) section in this Policy.

[Back to TOC](#)

**3.1.2 Changing or Updating the User-ID**

User ID change requests must be processed via the Company Name Change website at <https://directory.accenture.com/namechange>. Users are only permitted to change their user ID in accordance with the [Accenture Enterprise ID standard](#).

Refer to Company [Policy 0053 – Non-Company Access to Company Systems](#) for information on changing or updating a contractor user ID.

[Back to TOC](#)

**3.2 Authentication**

There are currently two authentication mechanisms used in the Company environment: password-based and token-based. The predominant one is password-based authentication; however, the Company is moving toward token-based authentication for applications containing "Secret" data as defined in the [Data Classification & Protection Standard](#) and for remote access into the Company network. When granted access to a system, users will be instructed on how to log into the system. Additional information, on protecting passwords and passcodes can be found in the [Identification & Authentication standard](#)

Access rights should be provided based on the Principle of Least Privilege as defined in the [Access Control standard](#).

## 5.0 Privacy

### 5.1 Expectation of Privacy

The workstations, laptops, and user accounts (e.g. user IDs and authentication mechanisms) are given to Company users to enable them to perform their jobs. However, users should not have an expectation of absolute privacy in the materials that are created, sent, or received by them on Company systems. To the extent permitted by local laws and regulations, Company authorized personnel (such as Information Security team members, Computer Incidence Response Team (CIRT) personnel, and technology support personnel) may examine all material stored on Company systems without prior notice. Examples of situations may include investigation for a suspected breach of security, or for the prevention or detection of crime, and other legally permissible situations. For more information regarding data privacy, refer to [Policy 0090 – Data Privacy](#).

### 5.2 Monitoring of Computer Usage

Subject to local laws and regulations, the Company may monitor any aspects of its computerized resources, including, but not limited to, monitoring sites visited by users on the Internet, monitoring chat groups and newsgroups, reviewing material downloaded from or uploaded to the Internet by Company users, and reviewing e-mail sent and received by Company users.

Wherever possible, monitoring will be carried out by methods which prevent misuse, such as automated monitoring software. The Company may use automated monitoring software to monitor material created, stored, sent or received on the Company network to ensure that inappropriate material is not created on or transmitted via Company systems.

[Back to TOC](#)

## 6.0 Confidentiality

Users of Company systems are granted access to a wide variety of data, including Company internal data (e.g., financial information, personnel information, etc.), client data, and alliance partner data. Sensitive data must be protected to ensure that it cannot be viewed or actively accessed by unauthorized persons. To protect all confidential information follow the requirements outlined in the [Confidentiality Standard](#). When handling client or other third-party data, users will adhere to the confidentiality requirements outlined in the [Confidentiality Standard](#). Company people and Company-hired contractors must comply with written confidentiality agreements and acceptable use policies provided by the client. If the written Confidentiality Agreement between the Company and the client or other third party provides additional or more stringent measures, that Agreement will supersede the requirements in the standard. Prior to sending client information outside of the client's organization, Company people and Company-hired contractors must be aware if the client explicitly prohibits communication over public computer systems (e.g., government).

[Back to TOC](#)

### 7.0 Required Security Behaviors for Acceptable Use

#### 7.1 Acceptable Use of Company E-mail

Company e-mail accounts are provided to Company users primarily for business purposes, although limited personal use is acceptable. All Company employees are expected to exercise good judgment and act in a professional manner in email correspondence. Employees should always use language that reflects positively on themselves and the Company. Company e-mail is not to be used for frequent or continuous personal needs, or to conduct business that is not Company-related. For example, a Company e-mail account should not be used for personal newsletters, personal internet purchase confirmations, personal banking accounts, etc. Instead personnel should obtain a personal e-mail such as hotmail or yahoo for non-business communications.

All users must immediately open and act upon security communications from *Protecting Accenture*. Users should not open e-mail attachments or click on URL links in the e-mail if the sender is unknown, or if the file type is unfamiliar, without confirming the contents of the attachment with the sender. Users should be cautious with e-mails from trusted sources that appear out of character for the sender. Users should contact the sender to ask about the validity of the e-mail before opening any attachments.

A chain e-mail is a message sent to a number of people asking each person to send the message to other people to receive some benefit or avoid a negative occurrence. Company users are strictly prohibited from initiating or forwarding chain e-mails using their Company account or from a Company workstation or laptop. Users must immediately delete any chain e-mails that they receive from others.

Spam is any unsolicited, non-business related e-mail, including chain e-mails, or offensive material. Users must not respond to or forward Spam to others. Users should delete spam without opening the message. For more information on avoiding spam, review the solution provided on eSupport.

Company users may not use any techniques to modify the "From" line or other sender/origin information in e-mails to change, hide, or disguise their identity. Use of the Company mailer for business purposes is acceptable. Sending anonymous or pseudonymous electronic communications is not allowed. Sending e-mails on behalf of someone else (e.g., an executive assistant sending an e-mail on behalf of an executive), when this is indicated in the e-mail, is acceptable.

To protect the Company environment from potentially harmful viruses that can be introduced by third party Internet Service Provider accounts and/or client accounts, users are prohibited from adding other mail accounts (e.g. POP3, IMAP, and HTML, etc.) to the standard Company Outlook client profile. Users must create a separate Outlook client profile for third party mail accounts.

#### 7.2 Acceptable Use of Client E-mail

Client projects or outsourcing arrangements may require Company personnel to communicate using an e-mail account on their system. Use of a client's or outsourcer's e-mail account will only be allowed if required by the client to provide the service or solution that the Company was engaged to deliver, and a Non-Disclosure Agreement (NDA) is in place. It is the responsibility of the client partner to ensure that the appropriate NDA is in place, and that the client abides by it. Company personnel should follow these steps when using a client e-mail account.

- Company personnel using a client-issued e-mail account should limit their use of this account to the client project-related work. Company confidential or proprietary information as well as another client's information should not be discussed using a client e-mail account.
- Company personnel should clearly identify themselves as a Company employee when using the client e-mail account to communicate.
- Company personnel should not use the client e-mail account to engage in illegal activities or to send spam mail.
- Company e-mail must not be automatically forwarded outside of the Company's control, such as to the Internet or client e-mail systems. The only allowable exception is for those users with an eID. Where eID users will have Company e-mail forwarded to a client machine, Company client partners must ensure that such e-mail will be properly protected while in the client's custody.
- Company personnel must familiarize themselves with the client's "Acceptable Use of E-mail" policy and abide by it.

#### 7.3 Acceptable Use of Company Resources

The Company provides many resources to employees, such as Internet access, which is for business use, although limited personal use is acceptable. Company resources should not be used to conduct any activity which is illegal (e.g., gambling, surfing/downloading child pornography, violating copyright) or to conduct any activity which is inappropriate (e.g. sexually oriented, pornographic, harassing, discriminatory, obscene, libelous, defamatory, etc.). The following are some examples of activities that are considered misuses of Company resources:

- Using Company resources for extensive personal use.
  - Surfing the Internet on Company time to buy or sell personal goods.
  - Conducting prolonged conversations with friends or family via e-mail or Instant Messenger.
- Using Company resources to conduct illegal activities.
  - Using Company resources to access, download, or distribute pornographic, obscene, defamatory, discriminatory, harassing, or other inappropriate materials of any kind.
  - Using Company resources to gain unauthorized access to Company's resources, or the resources of other companies or entities (e.g., government).
  - Using Company resources in such a way as to incur lawsuits or other liability against the Company (e.g. by violating copyright/licensing laws, creating and distributing false financial information, or making defamatory allegations).
  - Violating the Acceptable Use Policies of a service provider whose services are being accessed via a Company resource.
- Using Company resources inappropriately.
  - Inappropriately disclosing Company data.
  - Posting Company memos to any non-Company site.
  - Using Company resources to conduct business for another company or organization when that business is not part of a client engagement or business development activity.
  - Sending inappropriate unsolicited e-mail (spam) to anyone. This also applies to users who affiliate themselves with the Company, but are using non-Company owned resources.
  - Using Company resources to publicly embarrass Company people, or to jeopardize the reputation of the Company (e.g., by transmitting libelous, slanderous, defamatory, threatening, abusive or other inappropriate messages).
  - Installation or use of peer-to-peer file sharing networks such as KaZaa, unless instructed by CIO Technology Services.
  - Using Company resources to download shared or pirated music, video files or software.

[Back to TOC](#)

#### 7.4 Using Instant Messaging Securely

As Instant Messaging tools are not secure, users should never click on a URL link sent via instant messenger if it appears unfamiliar or out of character for the sender. Users should contact the sender of any link that appears suspicious, and ask about the validity of the link before attempting to access the site. In addition, files received via instant messenger must be scanned with a virus scanner prior to being opened or executed. Finally, users should never discuss or send unencrypted files containing confidential information via instant messaging tools.

#### 7.5 Virus Prevention Responsibilities

Computer viruses can cause substantial damage to Company systems and data. All Company laptops and workstations have Symantec AntiVirus software installed on them. Users may not disable Symantec, prevent its automated updates or scans, or reconfigure it in such a way that the functionality is decreased, unless instructed to do so by an [authorized CIO Technology Services, local technology support, or Computer Incident Response Team \(CIRT\)](#) person. If a client project requires the use of an alternative antivirus software, the project must apply for an exception. To apply for an exception clearly document the business reason and submit it to the [Security Exceptions site](#) for evaluation and approval.

Users are responsible for opening and immediately acting upon *Protecting Accenture* or CIO Technology Services virus alerts. Materials received from external sources on any removable medium, or downloaded from the Internet or from networks that do not belong to the Company, must be scanned for viruses upon receipt, prior to being used or forwarded on Company networks or computers. If a user discovers a virus on their computer, or inadvertently introduces a virus into the Company environment, that individual must contact CIO Technology Services or the local technology support provider immediately.

[Back to TOC](#)

#### 7.6 Backup Responsibilities

Company users are responsible for regularly backing up their laptop or workstation data with the utilities provided to prevent data loss. In the case of permanent disk failure or theft, a backup will be the only means of recovering essential data.

Company users are also responsible for adequately protecting the backup media in their possession. If sensitive data was placed on a backup medium, that medium must be stored in a secure location, such as a locked drawer or cabinet. Backup media with sensitive data must not be shared with other users. Once the medium is no longer needed, it must be destroyed prior to being discarded, in accordance with [Policy 0123 – Global Archives and Records Management](#).

#### 7.7 Maintaining Company-Provided Security Tools

In addition to anti-virus software, the Company provides users with a variety of other security tools. Examples of security tools include Internet Security Systems' RealSecure Desktop Protector personal firewall, Symantec AntiVirus software, Accenture Active Update software, Accenture Connection and a number of Windows security configurations. Users must maintain Company-provided tools in good working order by acting upon Protecting Accenture or CIO Technology Services communications containing upgrades, patches, and other maintenance tasks. Users are not permitted to disable Company-provided security tools or to reconfigure them in any way that would decrease their functionality, unless instructed to do so by an authorized CIO, or [Computer Incident Response Team \(CIRT\)](#) person.

[Back to TOC](#)

#### 7.8 Rebooting Company Provided Computers to Obtain Security Patches

Company laptops and workstations must be completely powered down and rebooted at a minimum of once per week. Security patches distributed to Company computers frequently are not implemented until a reboot of the system has occurred.

#### 7.9 Legal Notice

Company laptops and workstations are configured to display a legal notice, notifying the user that the Company system is to be used for authorized purposes only. Users are not permitted to disable this notice from their computers.

[Back to TOC](#)

#### 7.10 Acceptable Use of Non Company Owned Machines

When accessing Company data from a non-Company owned machine, users must not introduce new security threats into the Company environment or prevent unintended disclosure of sensitive Company data. The following requirements must be followed when using a computer not owned by the Company to access Company resources:

- Any Non Company machine connecting to the Company network via VPN or the Company LAN, must follow the Non Company Workstation Standard.
- Public computers such as Internet Cafes and airport kiosks should only be used to connect to Company resources when there are no other options available and for emergency reasons. Users must not use Instant Messaging to discuss Company or client business on a public kiosk machine.
- Users should never use Microsoft's "save password" functionality on non-Company owned machines.
- Users who entered their Company Enterprise ID and password on a public, client or any other non-Company owned machine to access resources, must change their Enterprise Password the next time they log on using their Company computer.
- Users must be aware that if they launch or view any e-mail attachments on a public machine, a copy of the attached document will be saved to the machine's hard drive. If it is necessary for the user to view a document on a public machine, the user must use the computer's search facilities to locate and permanently delete any copies of the document that were saved to the machine's hard drive. Typically, attachments are saved to the computer's TEMP directory.
- Users that utilize a client-owned machine must ensure that all Company data is removed from that machine prior to submitting it to the client support team for service and prior to leaving the project or assignment.

[Back to TOC](#)

#### 7.11 Connecting to a Client Domain

In many client environments, Company people need to connect to the client's domain to perform the work for which they were engaged. Users should be aware that when their laptops are connected to a client domain, the client's system administrators have access to data on the laptop. Connection of Company machines to client domains will only be allowed if required by the client to provide the service or solution that the Company was engaged to deliver, and a Non-Disclosure Agreement (NDA) is in place.

It is the responsibility of the client partner to ensure that the appropriate NDA is in place, and that the client abides by it. It is the responsibility of the user to remove any information about other clients, and any Company highly confidential or secret data from their laptop prior to connecting to a client domain.

[Back to TOC](#)

#### 7.12 Copyright and Intellectual Property Regulations When Installing Non-Standard Software

Non-standard software is not supported by [CIO Technology Services](#) or the [local technology support provider](#). Non-standard software installed on Company computers must be installed with the latest security patches. The user must monitor the vendor for additional security patches and apply them. Users should not install software from unknown vendors that may provide little or no ongoing support for the software.

The user is responsible for obtaining a proper, paid license for any non-standard software installed on a Company machine. Non-standard software must be properly licensed. Company users must comply with all software licenses, copyrights, and all other local laws and regulations governing intellectual property and online activities. Software installed on Company computers that violate copyright laws or licensing agreements exposes the Company to legal and commercial risk. By definition, anything posted on the Internet that is an original work (including e-mail, pictures, jokes, artwork, music, etc.) is protected by copyright law(s), whether or not it is explicitly indicated that the work is copyrighted, or the copyright (©) symbol is included. Therefore, users may not use such original works of authorship (e.g., by using "cut and paste" or "copy and paste"), or download music or videos without the author's (or artist's) express permission. In a text-based document, merely changing a few words is not enough to avoid copyright infringement issues. If a copyright law is violated using Company resources, the Company can be implicated as a distributor. Refer to [Policy 0059 – Software: Acceptable Use](#) for details on software installation and licensing agreements.

Users that are unsure if a piece of software is non-standard should contact [CIO Technology Services](#) or the [local technology support provider](#).

#### 7.13 Copying Software

The software on the Company network was purchased under license agreements with the manufacturers, and is protected by national and international copyright laws. These licenses and copyrights limit each user's rights to copy, distribute, and use the software. Unless otherwise documented in the license agreement, Company users may not copy or distribute software from the Company network without prior written approval from the software's manufacturer (reference [Policy 0059 – Software: Acceptable Use](#) for additional information).

[Back to TOC](#)

If a security incident is suspected or the user is aware of any violations to security policies, the user must immediately notify [CIO Technology Services or the local technology support provider](#), who will notify the Company [Computer Incident Response Team \(CIRT\)](#). Users affected by a possible security breach must not make any changes to their computers unless notified by a CIO Technology Services or CIRT representative, or until authorized security personnel have gathered any evidence they may need. If a user is ever in doubt as to the security relevance of their circumstance, the user should contact CIRT and verify.

[Back to TOC](#)

#### 8.0 Communication of Trade Secrets

Unless expressly authorized by senior executives, sending, transmitting, or otherwise disseminating Company confidential or secret data or Company's clients' proprietary, secret, or other confidential information is forbidden. Unauthorized distribution of such data may result in significant civil liability (reference [Policy 0051 - Use and Distribution of Packaged Knowledge](#) and [Policy 0091 - Intellectual Property](#)).

Users must always remember that unencrypted e-mail, unencrypted instant messenger conversations, and the Internet are insecure means of communication. Users may never send Company or Company client proprietary, confidential or trade secret information without first getting the appropriate approval from senior management, and encrypting it with Company-approved cryptographic technology.

[Back to TOC](#)

#### 9.0 Disclaimer of Liability for Use of the Internet

Users are cautioned that accessible Internet content may include offensive or otherwise inappropriate material (e.g., sexually explicit, discriminatory, etc.). If unintentional contact with this material occurs, users must navigate away from the content or close the browser window. The Company is not responsible for the content of Internet material viewed or downloaded by users.

##### 10.0 Physical Security

#### 10.1 Laptop and Wireless Device Protection

Users are responsible for protecting their laptops and wireless devices from unauthorized access and theft at all times (including but not limited to while in the office, at the client site, or in a hotel). In addition to protecting data on the computer screen as described in this Policy, all laptops must be secured with lockdown cables, and all wireless devices must be kept out of sight in a secure location (e.g., locked cabinet or drawer). Users must never leave laptops or wireless devices unattended (even laptops with a lockdown cable), in populated public places such as airports or subways, or in the checkrooms of hotels or restaurants. Furthermore, laptops and wireless devices must never be checked on an airplane as baggage; they must be carried onto the aircraft. It is strongly recommended that laptops and wireless devices never be left in automobiles, as automobiles are theft-prone locations. However, if extenuating circumstances arise where a laptop or wireless device must be left in an automobile, it must be locked in the trunk, out of sight.

In the case of laptop theft, users must immediately report the theft to [CIO Technology Services or the local technology support provider](#).

#### 10.2 Desktop Protection

In addition to protecting data on the computer screen as described in this Policy, all desktop computers that provide the capability must be secured with lockdown cables.

[Back to TOC](#)

#### 10.3 Printed Materials and Storage Devices

Sensitive printed material must be removed from the printer immediately after completing the printing process. Users are responsible for protecting all physical devices (laptops, PDAs, CDs, Jaz disks, USB keys, tapes, etc.) containing sensitive information to avoid unauthorized or unintended disclosure (e.g., keep them locked up, do not leave them unattended on a desk, in public places, or at the client site, etc.).

NOTE: Even if data has been deleted from a magnetic medium (such as a tape or floppy disk), it can still be recovered. Therefore, users may not share magnetic media that contain stored sensitive data. If such a medium is no longer needed, it must be destroyed and discarded, in accordance with [Policy 0123 - Global Archives and Records Management](#).

[Back to TOC](#)

#### 10.4 Security Devices

As the Company and its clients expand their security capabilities, users may be given ownership

of certain security devices that require protection. This may include tokens, smart cards, smart card readers, or other devices. Such devices may not only have a significant financial value, but they also provide access to Company or client systems when coupled with a PIN or password. These devices must be protected from loss, theft, and damage, and must never be shared with others.

[BACK TO TOP](#)

#### SUPPORTING DOCUMENTATION

The following examples and/or frequently asked questions have been provided to help illustrate the implementation of this Policy.

[F](#)

The following is a list of documents that support this Policy. Click on the name of the document to view the content.

[F](#)

[BACK TO TOP](#)

#### SUPPLEMENT(S)

There are no supplements to this policy.

[BACK TO TOP](#)

#### CONTACT INFORMATION

##### General Policy Questions

Questions related to this Policy can be sent to Katherina Page

IE-mail: [katherina.page@accenture.com](mailto:katherina.page@accenture.com)

Katherina Page – Octel: 45/51331; Phone number: +1 (513) 455-1331

##### Technology Questions or Assistance

Technology support is available online at eSupport: <https://esupport.accenture.com/>. Worldwide support phone numbers for CIO Technology Services and local technology support providers are available at: <https://cio.accenture.com/support.asp>.

##### Computer Incident Response Team (CIRT)

CIRT is responsible for investigating computer security related incidents. For general questions to CIRT:

E-mail: [CIRT1@accenture.com](mailto:CIRT1@accenture.com)

To speak with a CIRT representative, please call the CIRT hotline at +1 (312) 737-2478. If no one is available to answer the call, you may leave a message which will page someone to call you back.

For emergency, 24-hour support, or if you need to call collect, please call the Asset Protection hotline at +1 (202) 728-0645.

##### Legal Questions

Questions regarding intellectual property rights, copyrights, and other similar legal matters should be sent to the Legal and Commercial Intellectual Property mailbox:

E-mail: [ip.legal.mailbox@accenture.com](mailto:ip.legal.mailbox@accenture.com)

##### Security Exceptions Mailbox

Exceptions must be documented and approved. Please submit an exception via the [Security Exception Website](#).

[BACK TO TOP](#)

#### BACKGROUND/RATIONALE

This policy provides those security measures that are specifically applicable to end users, and describes behaviors that are required to maintain those measures. NOTE: all Company people, as well as any third parties that require access to Company systems

(e.g., contractors, clients, affiliated company personnel, etc.), are end users, and are responsible for compliance.

[BACK TO TOP](#)

Related Terminology:

Copyright 2001-2005 Accenture. All Rights Reserved. Accenture Confidential. For Internal Use Only. [Terms of Use/Privacy Statement](#)

U.S. DATA PRIVACY COMPLIANCE CONSENT FORM

I acknowledge that I have read the Accenture data privacy policy (the "Policy"). I consent to the processing of personal data relating to me in accordance with the Policy.

In particular, I consent to:

- a) the processing of sensitive personal data about me to the limited extent, and for the purposes, described in the Policy; and
- b) the transfer worldwide of personal data held about me by Accenture to other employees and offices of Accenture's worldwide organization and to third parties where disclosure to such third parties is required in the normal course of business or by law.

The references to information "relating to me" or "about me" include references to information about third parties such as my spouse and children (if any) which I provide to Accenture on their behalf. The reference to "sensitive personal data" is to the various categories of personal data identified by European and other data privacy laws as requiring special treatment, including in some circumstances the need to obtain explicit consent. These categories are outlined in the accompanying memo. I will treat any personal data to which I have access in the course of my employment in accordance with the Policy and the other Accenture policies and procedures. In particular, I will not use any such data other than in connection with and to the extent necessary for the purposes of my employment.

By this document, Accenture also discloses to you that a consumer investigative report may be obtained for employment purposes at any time during your employment. This report may contain information bearing on your credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or from public record sources or through personal interviews with your neighbors, friends or associates. Should an investigative consumer report be requested, you will have the right to ask for a complete and accurate disclosure of the nature and scope of the investigation requested and a written summary of your rights under the Fair Credit Reporting Act.

Please sign below to signify that you have received and understand the foregoing disclosure.

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Print Name

\_\_\_\_\_  
Date

\_\_\_\_\_  
Personnel Number

\_\_\_\_\_  
GMU/LMU