Motorola Information Protection Policy and Control Standards for Information Users

Effective Date 01 Jan 2007

Please submit questions to iProtect@motorola.com

PURPOSE

This policy communicates management's responsibility and establishes control standards for ensuring that risks to Information Assets and Information Resources are managed in alignment with business goals and in accordance with legal and regulatory requirements and professional standards.

SCOPE

This policy applies to all Motorola employees and third party contractors, consultants, service providers and any other third parties worldwide who have access to, or otherwise use, Information Assets and Information Resources. This policy applies during or outside normal business hours, and whether access to Information Assets or Information Resources occurs at a Motorola facility or other locations. It applies to all Information Resources that may contain Information Assets and/or are used in support of Motorola business, whether managed by Motorola or a third party.

CONTENTS

5.0 APPENDICES

ASSOCIATED CONTROL STANDARDS
Appropriate Use of Information Resources
Information Classifications and Safeguards
Responsibilities of Information Users
Privacy

1.0 DEFINITIONS

1.1 **Information Asset** means any information, tangible or intangible (physical or digital), that is owned by or created by Motorola, or is entrusted to Motorola by a third party, regardless of classification or value.

1.2 **Information Resource** means technology hardware (e.g., computers, servers, personal digital assistants, phones, networks, routers, accessories, storage media) and the software supporting the hardware (e.g., operating systems, databases, applications, services) owned by, leased to, or otherwise operated by Motorola.

1.3 **Information User** means anyone with access to Information Assets.

1.4 **Standard** means a detailed requirement that specifies the measure(s) by which compliance to a policy will be assessed.

2.0 STATEMENT OF POLICY

2.1 Motorola must maintain information protection safeguards to appropriately ensure that Information Assets and Information Resources sustain appropriate availability, confidentiality, and integrity.

2.2 Business and functional management must implement, support and comply with Motorola information protection policies, standards, and procedures.

2.3 Motorola Information Protection Services must maintain an Information Protection Framework consisting of policies, standards, architectures and practices. The Information Protection Framework provides a consistent communication of control standards that enable appropriate protection of Information Assets and Information Resources in accordance with applicable legal and regulatory requirements and professional standards.

2.4 The following Information Protection Standards are incorporated into this policy:
2.4.1 Appropriate Use of Information Resources
2.4.2 Information Classification and Safeguards
2.4.3 Responsibilities for Information Users
2.4.4 Privacy

2.5 Oversight for Motorola information protection is the responsibility of the Motorola Information Risk Board, which is accountable to the CEO and the senior leadership team. Motorola Information Risk Board members include senior management representation from Information Technology, Corporate Controller, Law, Human Resources, Supply Chain and business unit management.

2.6 Information Users must, at all times, comply with the Information Protection Policy, standards and procedures and other applicable Motorola policies.

2.7 Appropriate disciplinary or other action, in accordance with Motorola policies and applicable law, and/or legal action will be taken against individuals found to have violated this policy. Such action may include termination of employment or contract.

3.0 ROLES & RESPONSIBILITIES

3.1 Information Risk Board

- Evaluates risks that may potentially impact Motorola Information Assets and Resources, and determines the appropriate mitigation. Makes recommendations to the CEO for mitigation decisions that cannot be handled at the business level.
- Reviews self-assessment findings and independent audits regarding compliance with the Information Protection Policy, standards and procedures.

- Periodically reports on the status of risk mitigation and open risk issues to the Motorola Senior Leadership Team.

3.2 **Information User** – Complies with Motorola Information Protection Policy, standards and procedures, and reports suspected information protection incidents.

3.3 **Motorola Information Protection Services –** Maintains an Information Protection Framework consisting of policy, standards and practices.

3.4 **Management** – Implements and maintains information protection safeguards to ensure Information Assets sustain appropriate availability, confidentiality and integrity in order to facilitate reliance on Information Assets to meet business objectives.

4.0 REFERENCES

This policy is complemented by other Motorola policies and procedures, which include, but are not limited to, the following:

4.1 Code of Business Conduct (located at http://ethics.mot.com)

4.2 Human Resource Policies, including Progressive Discipline and Safe and Respectful Workplace (located at http://my.mot.com/go/hr)

4.3 Information Protection Framework (located at http://my.mot.com/go/informationprotection)

4.4 Motorola Record Management Policy (located at http://records.mot.com)

5.0 APPENDICES

5.1 Approval Authority and Issuance & Revision History

	Person	Function	Person, Title or Team
Policy Originator:	Bill Boni	Motorola Information Protection Services	CVP, Information Protection & Security
Reviewed By:		Law Department	Policy review team
Approved By:	Patty Morrison	Information Technology Department	CIO

Issuance/Revision History

Effective Date of Change	Revision Number	Reason for Change	Anticipated Date of Next Review
04-Dec-2006	1.0	Initial version (replaces SOPs E-60, E-62, E68 and E-69)	1-Nov-2007

---

iProtect
Think. Protect. Win.

Appropriate Use of Information Resources

These standards are elements of the Motorola Information Protection Policy
Report created 03 Nov 2006

Motorola Standard Title	Motorola Standard	Motorola Standard ID
Appropriate Use of Information Resources	Motorola Information Resources are provided to support Motorola's business objectives. Motorola employees and authorized third parties are permitted to use Motorola Information Resources only for approved purposes. Motorola Information Resources must be used in a professional manner, and such use must comply with all applicable policies and procedures, including, without limitation, the Code of Business Conduct, Human Resource policies, employee handbooks, non-disclosure agreements, and applicable laws and regulations. Occasional personal use of Motorola Information Resources is permitted if such use does not interfere with work responsibilities and other required business activities, business operations, or system performance. Any personal use of Motorola Information Resources must also comply with all applicable policies and procedures, including, without limitation, the Code of Business Conduct, Human Resource policies, employee handbooks, non-disclosure agreements and applicable laws and regulations. Where Motorola Information Resources are used for an occasional personal use, Motorola is not responsible for protecting personal information stored on or transmitted through Motorola Information Resources. Examples of Appropriate and Inappropriate Use Examples of appropriate non-business use of Motorola's Information Resources include, without limitation, the following: • Support of approved volunteer work in the community • Doing homework for a continuing education course • Conducting on-line banking and other personal financial transactions • Doing on-line shopping Some examples of inappropriate use of Motorola's	MOTCS-065

Information Resources include, without limitation, the following:

- Disclosing information that is owned by Motorola, or entrusted by a third party to Motorola, to unauthorized recipients
- Discussing on public forums Motorola Internal or Motorola Confidential Restricted information, including but not limited to, financial results or projections, future business plans, future or unreleased products, prospects, pending partnerships, our customers, or our share price, or commenting on rumors.
- Enabling non-Motorolans who have not signed the proper non-disclosure agreements with Motorola to access a Motorola provided network connection.
- Misusing intellectual property (e.g. trademarks, copyrights, or patents) of Motorola or a third party
- Communicating information that could be perceived as official Motorola positions or endorsements without proper management approval
- Communicating in ways that disparage Motorola's products or services
- Communicating in ways that disparage other companies' products or services (excluding objective reports of substantiated fact with limited internal distribution)
- Creating, storing, viewing or communicating content that is threatening, intimidating, discriminatory, or harassing to others, or is defamatory, obscene, profane, pornographic, illegal, slanderous, libelous, abusive, derogatory, threatening, racist, sexist, offensive, unlawful, or that may give rise to any civil or criminal liability under any applicable law, is strictly prohibited
- Appropriating, disclosing, accessing, distributing, storing, collecting or processing any Personal Information in violation of data protection or privacy laws
- Participating or engaging in activities that

	violate the law, the Code of Business Conduct, or any Motorola policy, standard or procedure • Originating or distributing chain letters or other mass mailings • Misrepresenting an individual's identity or the source of communications or information • Attempting to break into or monitor any Information Resource without proper authorization, whether within Motorola or another organization • Accessing Motorola Confidential Restricted and similar non-Motorola information on Information Resources without authorization • Promoting personal political or religious positions to fellow employees • Operating or otherwise supporting a personal business • Soliciting on behalf of charitable, commercial, or internal organizations, or otherwise, except as provided by appropriate Motorola HR policies/procedures on solicitation and distribution • Export or import of any government controlled information or software to or from unauthorized locations or persons without appropriate licenses or permits	
Adhering to Copyright Laws and Software License Agreements	Motorola employees, third party contractors and vendors must adhere to all copyright laws and packaged software license agreements. Packaged software products may only be duplicated in accordance with license agreements (e.g., a backup copy for protection). The use of copy protection bypass software is prohibited.	MOTCS-123

Unauthorized Software	Software that has been illegally copied, obtained from an unauthorized or untrusted source, or is designated as prohibited is not authorized for use on Motorola's Information Resources. Unauthorized software includes, without limitation, the following categories (unless limited usage is specifically permitted by another control standard, reference guide or approved procedure): • Adult/sexually oriented games and applications • Applications with functionality or end user license agreement (EULA) terms that conflict with Motorola policy, procedure, or safe computing standards. As an example, some "click through" agreements grant third parties unrestricted remote access to Motorola Information Resources and prohibit removal of the software once it is installed. Users must not install such software. • Data hiding (steganography) software • Data destruction software, if used to remove evidence of inappropriate use of Motorola Information Resources. Recommended usage is described in Protecting Information on Electronic Devices Reference Guide. • Distributed/grid computing applications (used to distribute resource intensive computing tasks across many systems) if they would make Motorola Information Resources available to third parties or non-Motorola networks • Encryption software, if used to hide evidence of inappropriate use of Motorola Information Resources. Recommended usage and approved tools are described in the Encryption Reference Guide. • Key logging/spying applications • Peer-2-Peer file sharing applications • Personal firewalls, other than those provided by the Information Technology department • Proxy or tunneling software that allows anonymous web surfing or enables reverse tunneling into the Motorola network from an external network, or otherwise circumvents	MOTCS-221

	firewalls, intrusion detection sensors or other safeguards • Remote management and remote screen viewing applications, unless provided by the Information Technology department • Software license key generators used to create unauthorized license keys, credit card numbers, passwords, and the like • Software that is prohibited by the Information Technology department, as described in the Class D list at desktop.mot.com/softwarestandards	
Restrictions on Personal Web Sites	Motorola employees and authorized third parties must not publish personal Web sites on Motorola Information Resources.	MOTCS-269
Restricted Use of System Audit Tools	Possession, distribution or use of network diagnostic, monitoring and scanning tools is limited to designated and authorized personnel in accordance with their job responsibilities. Approval for usage of such tools in production environments, including data centers, factories and the Intranet, may only be granted by Motorola Information Protection Services. Such tools may be used in lab networks that are isolated from the Motorola Intranet if authorized by the lab manager.	MOTCS-053
Use of Motorola-Provided Computers	All Motorola employees must use a Motorola provided (owned or leased) computer as their primary computer for conducting Motorola business. Exceptions must be approved by a business controller and a vice president of IT.	MOTCS-IPS0007
Right to Monitor and Audit Content on Motorola Information Resources	In accordance with applicable law, Motorola reserves the right to monitor, audit, access, search, inspect, and/or review the content of any electronic communication (e.g. email, instant messages, pager messages, text messages, voicemail, blogs, phone calls, etc.) and/or data created, stored, or otherwise transmitted on its computing resource(s) and/or network(s). This right extends to communications, programs, applications, and/or data created, stored, or otherwise transmitted for either a business or personal purpose. Motorola’s failure to monitor, audit, access, search,	MOTCS-230

	inspect, and/or review the content of any electronic communication and/or data created, stored, or otherwise transmitted on its computing resource(s) and/or network(s) in an individual instance or multiple instances does not constitute a waiver of Motorola's right to do so in other instances.	
No Expectation of Privacy or Confidentiality	Even though you may have a unique password that provides access to Motorola computing resource(s) and/or network(s), you do not have an expectation of privacy or confidentiality in any such electronic communication(s) or other data created, stored, or otherwise transmitted on Motorola computing resource(s) and/or network(s), except where required otherwise by applicable law.	MOTCS-IPS0009

Responsibilities of Information Users

These standards are elements of the Motorola Information Protection Policy
Report created 03 Nov 2006

Motorola Standard Title	Motorola Standard	Motorola Standard ID
Physically Protecting Laptops from Unauthorized Access	Laptop computers must not be left unattended or unsecured and must be locked or secured when there is doubt of the security of the physical environment. Laptops must not be checked in airline luggage systems, but must remain in the possession of the traveler as hand luggage at all times.	MOTCS-097
Use of Screen Savers	Users must not leave any Motorola Information Resource that contains Motorola information or is connected to a Motorola network unattended, and must logoff or activate a password protected screen saver program if the information resource is not used for a period of 30 minutes.	MOTCS-468

Use of User IDs	User IDs must not be utilized by anyone except the individual to whom the IDs have been issued. Users are responsible for all activity performed with their User IDs.	MOTCS-289
Using IDs Belonging to Others is Prohibited	Users must not perform any activities with User IDs belonging to others except for processing voice mail as described in MOTCS-274 "Securing Voice Mail Messages" under the Information Classifications and Safeguards section.	MOTCS-290
Recording Passwords	Users may record their passwords when they are changed if they are having problems memorizing a number of difficult passwords and if the media on which the password is stored is adequately secured using Enhanced Controls. This includes locking up the information when not in use.	MOTCS-307
Reporting Security Incidents	If any Motorola employee, contractor or service provider detects or suspects that a security incident has occurred or may occur, they must contact Motorola Information Protection Services at +1 (847) 725-4060 or http://mips.mot.com/ir. If any Motorola employee, contractor or service provider detects or suspects that an Information Resource has been compromised, they should immediately disconnect the affected Information Resource from the Motorola network and report the incident. Only authorized personnel are permitted to conduct an incident investigation or test the safeguards of a Motorola Information Resource. The following are examples of security incidents that must be reported: • Computer Fraud - Computer-related crime such as improper manipulation of input data, output results, application programs, data files, computer operations, communications computer hardware, system software, or theft of service • Malicious Code - A general name for programs intended to cause harm or otherwise defeat security measures. Examples include logic bombs, trap doors, Trojan horses, worms and viruses • Network Penetration - The attempted or successful act of bypassing the security mechanisms of a system without prior approval • Spamming - The sending of email messages from Motorola in violation of laws prohibiting unsolicited commercial e-mail • Unauthorized alteration or destruction of Motorola Information Resources • Theft or loss of any Information Resource • Theft or loss of any storage media that contains Motorola Confidential Restricted Information, Motorola records, intellectual	MOTCS-235

	property, proprietary information, Personal Information, and third-party information entrusted to Motorola • Unauthorized disclosure, alteration or destruction of Motorola records, intellectual property, proprietary information, Personal Information, and third-party information entrusted to Motorola	
Use of Public Domain Software	If public domain or mass-distributed programs (e.g., printer drivers) are required for a valid business need, the software must be obtained from a reputable source, such as a trusted vendor site. Software used for production must be tested in a development environment.	MOTCS-220
Installing Remote Control Software on Workstations	Remote control software must not be installed on user workstations except to support the remote administration of approved servers by Information Resource Administrators.	MOTCS-344

---

iProtect
Think. Protect. Win.

Information Classifications and Safeguards

These standards are elements of the Motorola Information Protection Policy
Report created 03 Nov 2006

Motorola Standard Title	Motorola Standard	Motorola Standard ID

Information Protection Classifications	Information Assets must be identified and classified at a level defined by an appropriate Information Authority. Information Assets may only be shared with persons authorized to have access; and who are under an obligation to maintain the confidentiality of the Information Assets. **Definitions:** • **Information Asset** means any information, tangible or intangible (physical or digital), that is owned by or created by Motorola, or is entrusted to Motorola by a third party, regardless of classification or value. • **Information Authority** means a business or functional vice president who determines and communicates which categories of information in his/her respective business/function are classified as Motorola Confidential Restricted and require Enhanced Controls. Alternatively, the Information Authority can be a security council appointed by the business president. • **Information Owner** means the person responsible for managing a particular Information Asset, regardless of what Information Resource contains the Information Asset. • **Information Resource** means technology hardware (e.g., computers, servers, personal digital assistants, phones, networks, routers, accessories, storage media) and the software supporting the hardware (e.g., operating systems, databases, applications, services) owned by, leased to, or otherwise operated by Motorola. • **Information User** means anyone with access to Information Assets. • **Intellectual Property** means trademarks or service marks, copyrights, patents, integrated circuit topographies, mask works, and any other materials considered intellectual property under the law of a respective country. • **Motorola Information** means any information owned by Motorola. The term does not include information entrusted to Motorola by a third party. Motorola retains ownership for all Motorola Information regardless of ownership of the Information Resource or media on which it is stored. • **Personal Information**, as defined in MOTCS-IPS0006, means any information that can be used to identify a person directly or indirectly. • **Motorola Proprietary Information** means Motorola Information relating to Motorola's business that is not generally available to the public, which impacts the production and sale of our products, improves our competitive position, or increases revenue and profitability. Examples include, but are not limited	MOTCS-024

to, the following:

- Consumer and customer lists
- Information pertaining to current or potential litigation
- Internal and external audit and information protection assessment reports
- Marketing and sales plans
- Mergers, acquisitions or divestitures activities
- New product or process development, including product designs and physical prototypes
- Strategic planning information and roadmaps
- Trade secrets
- Unpublished and internal financial statements and budgets

- **Third Party Proprietary Information** means information developed by a third party that has been classified by the third party as proprietary. It is protected in accordance with Motorola standards and with the terms of the particular agreement under which the information was disclosed to Motorola.
- **Resource Administrator** means individuals or groups of individuals responsible for implementing and/or maintaining an Information Resource at the request of an Information Owner.

Classification Levels:

Motorola Information Assets are classified in one of three categories: Public, Internal, and Motorola Confidential Restricted.

Public

Information Assets that Motorola freely discloses or shares with the public, for example:

- Approved press releases
- Published annual reports
- Published marketing materials

Internal

Information Assets used in day-to-day business operations are classified as Internal, unless designated as Public or Motorola Confidential Restricted by an Information Authority. Characteristics of Internal information are:

- Unauthorized disclosure of the information would not directly or indirectly have a significant, material adverse impact on

Motorola, employees or third parties.
- The information is not subject to regulations which require enhanced protection.
- The information is meant to be shared internally within Motorola as needed.

Examples include:

- General business correspondence
- Commonly shared (internal) information, including operating procedures, policies and interoffice memorandums
- Internal telephone directories

Control summary:

- Internal Information Assets are subject to Basic Controls. Access is determined by the Information Owner.
- Internal Information Assets may be disclosed to Motorola personnel on a "need-to-know" basis.
- Internal Information Assets may be disclosed to non-Motorolans on a "need-to-know" basis, provided appropriate safeguards are in place. Appropriate safeguards include, but are not limited to, executed contracts containing confidentiality provisions, such as a professional services agreement or a non-disclosure agreement.
- No information protection labels are required for internal distribution. The Information Owner is responsible for determining if special protection is required prior to sharing the Internal information with a third party. If special protection is required, this information must be reclassified as Motorola Confidential Restricted, and labeled and protected accordingly.
- Information Users who identify a misclassified Information Asset must notify the Information Owner.
- Other controls as noted in related control standards and practices/procedures

Motorola Confidential Restricted

Information that, if disclosed, compromised or destroyed, would directly or indirectly have a significant, material adverse impact on Motorola, its customers or employees. Motorola Confidential Restricted information is "data of concern" and has high confidentiality or integrity requirements. Characteristics of Motorola Confidential Restricted information are:

- Unauthorized disclosure of the information would directly or indirectly have a significant, material adverse impact on Motorola, its customers, partners or employees.
- Unauthorized disclosure of the information could expose Motorola to significant financial loss or embarrassment, or jeopardize the protection of Motorola's assets.
- Unauthorized disclosure of the information would violate an individual's right of privacy.

Examples include:

- Intellectual Property
- Personal Information
- Motorola Proprietary Information
- Third Party Proprietary Information entrusted to Motorola
- Information subject to regulations that require strong protection
- Specific information or types of information designated as Motorola Confidential Restricted by an Information Authority
- Non-Motorola Information Assets with intrinsic value or explicit labels similar to Motorola Confidential Restricted.
- Product prototypes which would expose trade secrets or other Motorola Proprietary Information upon examination.

Control summary:

- Motorola Confidential Restricted Information Assets are subject to Enhanced Controls. Access is limited to people with a "need to know" as determined by the Information Owner.
- Motorola Confidential Restricted Information Assets may be shared with parties who have an approved business "need-to-know". Any party receiving Motorola Confidential Restricted information must be covered by an executed contract containing appropriate confidentiality obligations, (e.g. a non-disclosure agreement).
- Third Party Proprietary Information may not be shared with other third parties without prior written authorization of the owning party.
- "Motorola Confidential Restricted" labels are required.
- Other controls as noted in related Motorola control standards and practices/procedure

Periodic Review of Information Classifications	Information Owners must annually review the classifications of Motorola Confidential Restricted Information Assets for which they are responsible in order to verify that the classification level is still appropriate. **Declassification** • Personal Information must retain the Motorola Confidential Restricted classification until the information is destroyed. • Non-Motorola Information Assets in Motorola's custody must retain the owner's classification and labels until the owner reclassifies the information or until such time as Motorola's obligations have expired (refer to the executed contract under which the Information Asset was provided to Motorola). • The Information Authority must establish guidelines for classification and declassification. • The Information Owner must declassify and re-label information per the classification and declassification guidelines. • Examples of declassification criteria are indicated in the examples below. **Classification and Declassification Examples** Intellectual Property Information: • Patent (upon granting) • Trademark (upon registration or public use) • Industrial designs and product designs (as defined by the Information Authority) • Marketing plans (as defined by the Information Authority) • Prototypes (upon public launch of product) • Trade secret data and source code (as defined by the Information Authority) Proprietary Information: • Periodic financial results (upon public release)	MOTCS-IPS0008

	Financials and budgets (as defined by an Information Authority) • Strategic planning (as defined by an Information Authority) • IT infrastructure (as defined by an Information Authority) • Internal and external audit and information protection reports (as defined by an Information Authority) • Non-public regulatory agency reports (as defined by an Information Authority) • Merger, acquisition or divestiture activities (until approved for public disclosure by an Information Authority) • Executive-level activities (as defined by an Information Authority) • New product and process development (as defined by an Information Authority)	
Users Must Protect Information Assets Based on Information Protection Classifications	Information Users are responsible for handling Information Assets with care commensurate to the information protection classification of that asset. All Information Assets must be protected with at least Basic Controls. Information that has been classified as Motorola Confidential Restricted must be protected with Enhanced Controls. Third party Information Assets in the custody of Motorola must be protected in accordance with the terms of the contract under which it was provided to Motorola. **Basic Controls** are the minimum controls that must be used to protect all Information Assets in order to provide reasonable/sufficient protection for Internal information. Basic Controls are defined by business and functional management and based on standard industry practices. **Enhanced Controls** are mandatory additional controls, beyond Basic Controls, that apply to any: • Information Assets designated Motorola Confidential Restricted, • Third-Party Proprietary Information Assets entrusted to Motorola, or • Information Assets that requires a high degree of confidentiality, integrity, availability or monitoring.	MOTCS-022

	Enhanced Controls include, but are not limited to, specific security architectures such as E-zones, encryption, and other manual, physical and technical security processes identified by Motorola Information Protection Services or Information Authorities to protect the information types listed above from the expected threat environment. Refer to the Guide to Safeguarding Information.	
Information Classification Labeling	**Labeling hardcopy and electronic documents** **Public information** No information protection labels are used. **Internal information** No information protection labels are required for internal distribution. The Information Owner is responsible for determining if special protection is required prior to sharing the Internal information with a third party. If special protection is required, this information must be reclassified as Motorola Confidential Restricted, and labeled and protected accordingly. **Motorola Confidential Restricted information** • Hard copy and electronic documents containing Motorola Confidential Restricted information anywhere in the document must be clearly labeled "Motorola Confidential Restricted" on every page, and include page numbers. • Oral disclosures of Motorola Confidential Restricted Information made to third parties must be followed up in writing summarizing the disclosure and stating that such disclosure is Motorola Confidential Restricted within 30 days of the disclosure. • Product prototypes which would expose Intellectual Property or Proprietary Information upon examination must be labeled. • Non-Motorola Information Assets entrusted to Motorola retain the owner's label (if any). **Legacy Motorola Information Classifications and Labels** Legacy labels should not be used on new documents. Legacy information labeled Motorola Confidential Proprietary or Motorola Registered Secret Proprietary does not need to be re-labeled "Motorola Confidential Restricted" except under the following conditions: • The information is revised or updated and falls under the	MOTCS-047

	definition for Motorola Confidential Restricted, or • The information will be disclosed to third parties. Equivalence of legacy labels: • General Business Information must be treated as Motorola Internal • Motorola Internal Use Only must be treated as Motorola Internal • Motorola Confidential Proprietary must be treated as Motorola Confidential Restricted • Motorola Registered Secret Proprietary must be treated as Motorola Confidential Restricted	
Users Must be Granted the Minimum Level of Access Required	Motorola's Information Owners and Information Resource Administrators must only grant the minimum level of access required for users to successfully complete their job functions.	MOTCS-330
Distributing and Encrypting Motorola Confidential Restricted Information	Motorola personnel, third party consultants, contractors and vendors are required to adhere to the following requirements with respect to the distribution of Motorola Confidential Restricted information in hard copy or electronic form: • A contract containing appropriate confidentiality obligations must be executed prior to the release of any Motorola Confidential Restricted information to a third party. • Motorola Confidential Restricted information may not be removed or sent from Motorola's premises unless there is a business requirement to do so. • The release of Motorola Confidential Restricted information to third parties requires prior written authorization by the originating department's officer level management. • Third Party Confidential Information may not be shared with other third parties without prior written authorization. • Personal Information about current and potential customers must be strictly controlled and used only for the business purposes specifically consented to by the data subjects. Disclosure of Personal Information to third parties must not take place unless required or permitted by law or authorized by the person whose Personal Information is being disclosed. • If Motorola Confidential Restricted Information is lost or disclosed to unauthorized parties, or is suspected of being lost or disclosed to unauthorized parties, Motorola Information Protection Services must be notified immediately.	MOTCS-IPS0002

	• Motorola Confidential Restricted information must be encrypted as described in the Guide to Safeguarding Information.	
Handling Information in Electronic and Hard Copy Form	Motorola personnel, third party consultants, contractors and vendors are required to adhere to the following standards with respect to the handling of Motorola Confidential Restricted information in electronic and hard copy form: • All hard copy documents that contain Motorola Confidential Restricted information must be securely handled at all times. Such information must be used in a controlled location where access is limited to personnel with a business "need to know". • All electronic media (data storage devices), such as computers, personal data communications devices, removable hard drives or other types of portable memory devices that contain information classified as Motorola Confidential Restricted must be securely handled at all times. Such media must be used in a controlled location where access is limited to personnel with a business "need to know". • Media containing Motorola Confidential Restricted Information must not be left unattended in automobiles, at home or in other public areas. • All electronic media must be handled so as to prevent damage due to exposure to extreme heat or cold, direct sunlight, extreme humidity and strong magnetic fields. When transporting backup media to a remote storage location, transportation must be performed by authorized personnel or a courier service. During movement, care must taken to safeguard the media from loss, damage or destruction from both human and environmental threats. • While conducting Motorola business, Motorola personnel may receive and use information belonging to external parties. Information entrusted to Motorola through contracts or agreements (including non-disclosure agreements) must be protected according to the terms of such contracts or agreements. Questions or issues concerning such contracts or agreements must be referred to the Law Department. • When transferring ownership of Information Resources, all media (e.g. hard drives, diskettes, cartridges, CDs, DVDs, tapes, SIM cards) and embedded non-volatile memory containing Motorola Confidential Restricted information and licensed software must be overwritten to ensure the data is unrecoverable or destroyed. This includes all external media that will remain with the device. • When Motorola personnel transfer to another department or leave the company, and when the work of a third party	MOTCS-IPS0003

	consultant, contractor or service provider is finished: • Motorola Confidential Restricted Information Assets, Third Party Confidential Information Assets, and Motorola Records must be transferred to the Motorola manager responsible for the activity, or his or her designee, so that they may be appropriately retained or disposed of under Motorola's Record Retention Policy. • Personal Information must be permanently disposed of according to MOTCS-045 under the Information Classifications and Safeguards section. • Motorola Information must not be sold or ownership otherwise transferred to a third party unless authorized by the originating department's officer level management. Refer to the Guide to Safeguarding Information.	
Mailing Information in Hard Copy Form	Motorola personnel, third party consultants, contractors and vendors are required to adhere to the following standards with respect to the mailing of Motorola Confidential Restricted information in hard copy form: • The mailing of Motorola Confidential Restricted Information Assets must be to a named individual and not to an office, title or location. • The sender must use inter-company mail services or a reputable outside mail/messenger service. • Motorola Confidential Restricted Information Assets must be wrapped or sealed in an envelope or container that is labeled according to the information's classification and addressed to a named individual. It must then be wrapped or sealed in a non-transparent envelope or container a second time, and labeled only with the name and address of the recipient and the sender. The mailing or transmitting of technical data, software and computer programs between countries may be governed by regulations. Consult the Export Control Officer at http://export.mot.com for advice about transporting hard copy media.	MOTCS-051

Secure Transmission of Motorola Confidential Restricted Information	Additional controls must be employed when communicating, transmitting, handling, labeling, copying and disposing of Motorola Confidential Restricted information by voice, fax or video systems, including but not limited to: • Informing conference or meeting participants of the classification level of the information to be discussed • Physically securing the location of conferences and meetings where Motorola Confidential Restricted information will be discussed	MOTCS-277
Securing Telephone Conversations	When making or receiving a telephone call, personnel are responsible for the confidentiality of their conversation. If Motorola Confidential Restricted information will be discussed, the identity of the receiving party must be verified. Telephone systems (i.e., wired and wireless) are not considered inherently secure, and therefore the following minimum safeguards should be considered to prevent unauthorized disclosure of Motorola Confidential Restricted information: • Ask who is participating in and listening to the call • Attempt to identify the participants by recognizing their voices or through introduction by people you know • Verify the caller's need to know the information you plan to discuss • Generate a subject-specific non-disclosure agreement through http://nda.mot.com and ensure that it is executed prior to the commencement of the call • Be cognizant of eavesdroppers	MOTCS-273
Securing Voice Mail Messages	Personnel are responsible for the confidentiality of their messages when reviewing or leaving voice mail messages. Voice mail systems are not considered inherently secure, and therefore the following minimum controls must be used to prevent unauthorized disclosure of Motorola Confidential Restricted information: • Delete/purge messages that no longer have value, in compliance with record retention procedures • Be cognizant of eavesdroppers • All mailboxes, fixed and mobile, must have passwords. Voice mail passwords must be protected just as any other password; however voice mail passwords may be disclosed to more than	MOTCS-274

	one person if there is a business justification for such disclosure. Examples include: • The mailbox is used by callers to reach a department or specific service and multiple people have the responsibility for retrieving and processing those messages or administering the mailbox. • An administrative assistant or other person has been given the responsibility for reviewing and responding to the messages by the mailbox owner. This could include someone providing temporary coverage for the owner of a mailbox while that person is away from the office.	
Securing Fax Communications	When sending or receiving a fax, personnel are responsible for the confidentiality of the information transmitted. Facsimile systems are not inherently secure, and therefore the following minimum security controls must be used to prevent unauthorized disclosure of Motorola Confidential Restricted information: • Verify fax numbers with the recipients • Use special features, such as mailboxes, when available • Place fax machines in an area where they can be monitored • Use cover pages to indicate authorized recipient(s) • Be present at the destination machine when receiving expected transmissions containing Motorola Confidential Restricted information	MOTCS-275
Securing Conference Calls and Video Conferences	When participating in conference calls and video teleconferences, personnel are responsible for the confidentiality of their conversations. Teleconference systems are not considered inherently secure, and therefore the following minimum controls must be used to prevent unauthorized disclosure of Motorola Confidential Restricted information: • Require passwords for access • Announce arrival and departure of call participant	MOTCS-276

Securing Meetings and Conferences	When participating in meetings and conferences, personnel are responsible for the confidentiality of their conversations. Meetings and conferences are not inherently secure, and therefore the following minimum security controls must be used to prevent unauthorized disclosure of Motorola Confidential Restricted information: • Ensure all participants have a need to know • Maintain and check an attendance list • Generate a subject-specific non-disclosure agreement through http://nda.mot.com and ensure that it is executed prior to the commencement of the meeting • Collect extra copies of handouts following the meeting/ conference • Distribute minutes securely and ensure the minutes are labeled as Motorola Confidential Restricted	MOTCS-278
Storing Information in Hard Copy Form	Motorola personnel, third-party consultants, contractors and vendors are required to adhere to the following guidelines with respect to the storage of information in hard copy form: • All information in hard copy form classified as Motorola Confidential Restricted must be stored in a secured room, in a locked filing cabinet or desk drawer that is accessible only by authorized individuals.	MOTCS-050
Disposing of Information in Hard Copy Form	Information Assets in hard copy form must be disposed of appropriately including compliance with Motorola's Record Retention Policy. • Motorola Confidential Restricted information and Third Party Proprietary Information entrusted to Motorola must be disposed of in a manner that ensures the information cannot be reconstructed into a usable format. Papers, slides, microfilm, microfiche and photographs containing sensitive information must be disposed of by cross-shredding or burning. • Documents containing Internal and Public information may be disposed of by recycling or normal trash disposal methods. • The use of third party collection and disposal services for disposal of information in hard copy form is authorized; however, care must be exercised in selecting suitable contractors that exercise adequate security controls.	MOTCS-052

Duplicating Information in Electronic Form	Copies of Motorola Information Assets and Third Party Information Assets entrusted to Motorola must be handled, and safeguarded following the same control standard requirements as original versions of the information.	MOTCS-041
Disposing of Information in Electronic Form	Information Assets in electronic form must be disposed of appropriately and in compliance with Motorola's Record Retention Policy. • All electronic media containing Motorola Confidential Restricted information and Third Party Proprietary Information entrusted to Motorola must be disposed of in a manner that ensures the information cannot be reconstructed into a usable format. Removable magnetic storage media such as disk drives and other portable memory devices that contain Motorola Confidential Restricted information or export controlled data must not be disposed of in regular waste containers. Magnetic media must be overwritten in such a manner as to cause the destruction of the sensitive data prior to reuse or being discarded. • Media containing Motorola Confidential Restricted information, Third Party Proprietary information entrusted to Motorola, or export controlled information, which cannot be overwritten, must be destroyed. • Defective or damaged magnetic storage media that contains Motorola Confidential Restricted information or Third Party Proprietary Information entrusted to Motorola must not be returned to the vendor who performs maintenance or repair, unless the vendor is contractually required to protect such sensitive data. The information must first be overwritten before the media may be released to unauthorized personnel. This also applies to media onto which an unsuccessful attempt has been made to copy sensitive information. Please refer to "Protecting Information on Electronic Devices" at http://compass.mot.com/go/dporg.	MOTCS-045

Privacy

These standards are elements of the Motorola Information Protection Policy
Report created 03 Nov 2006

Motorola Standard Title	Motorola Standard	Motorola Standard ID
Privacy Definitions	**Data Protection or Data Privacy** means the processing of Personal Information in compliance with applicable law and in accordance with Motorola's Privacy Standards. **Data Subject** means any individual natural identifiable person (e.g., employee, applicant, consumer, customer, supplier) associated with any Personal Information. **Data Subject's Consent** means any freely given specific and informed indication by which the Data Subject signifies agreement to how their Personal Information will be processed. **Personal Information** means information relating to a natural identifiable person ("Data Subject"), whether the Data Subject is an employee, employee family member, applicant, consumer, customer, supplier, or other partner or potential partner. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Personal Information includes both General Personal Information and Sensitive Personal Information. **General Personal Information** means, without limitation, the following types of information: names, dates of birth, U.S. Social Security Numbers (SSNs) and similar government/national identification numbers (including tax identification numbers), home and business addresses, home and business email addresses, home and business telephone numbers, employee ID numbers (e. g. Core ID, Commerce ID), credit card numbers, and passwords. **Sensitive Personal Information** means, without limitation, the following types of information: racial or ethnic origin, religious or philosophical beliefs, political affiliations/opinions, trade union membership, medical or health related records, sexual orientation, disabilities, and background checks.	MOTCS-IPS0006

	Processing of (or to Process) Personal Information means the processing of Personal Information in compliance with applicable law and Motorola Information Protection Standards. Processing means any operation or set of operations that is performed upon Personal Information, and includes, without limitation: collection, use, maintenance, recording, organization, storage, adaptation or alteration, retrieval, transmission, dissemination or otherwise making available, and/or disposal or destruction. **Record** means any recorded information that has value to the company for conducting its business or meeting its legal obligations. This includes information created or received in any form, including emails, paper documents, electronic documents, database or application information, and other electronic or photographic media. For additional definitions, please refer to the *Information Protection Framework Glossary*.	
Collection, Use, and Accuracy of Personal Information	Personal Information must only be collected and used in a lawful manner and for relevant and appropriate business-related purposes. For employees, this could include, but is not limited to, recruitment, administration of compensation and benefit programs, payroll, scheduling, training, performance management, succession planning, travel management, knowledge management, government compliance or employee/customer/public protection. For consumers and customers, this could include, but is not limited to, shipping ordered products, registering consumer warranties, repairing products, contacting customers in case of a product recall, providing promotional offers and other information in response to a request to receive such materials, disseminating newsletters, and receiving consumer comments and opinions. Personal Information must be processed in accordance with applicable local laws. Where required, Personal Information may be processed only with the explicit consent of the Data Subject. Motorola prohibits the use of more than four sequential digits of U.S. Social Security Numbers or similar government/national identification numbers as personal identifiers for Data Subjects, except where otherwise required by law, regulation, or other valid governmental authority. Motorola must, where required, inform Data Subjects of the category of information Motorola collects about them, the use of such information, the circumstances under which Motorola discloses Personal Information, including the types of potential recipients, the fact that Motorola employs privacy and information safeguards, and the circumstances under which	MOTCS-IPS0001

	Data Subjects may access, correct, amend, and/or delete their Personal Information Motorola must inform Data Subjects about our privacy principles, policies, and procedures. With certain exceptions, Motorola must provide Data Subjects with reasonable opportunities to access, correct, amend, and/or delete Personal Information that pertains to them. Data Subjects may be denied access to their Personal Information under certain circumstances, including: • Where access would involve disclosure of certain confidential or proprietary information (e.g., non-final reorganization or succession plans, non-final performance evaluations, proprietary consumer profiles, and credit risk scores); • In situations where granting access might be subordinate to the privacy interests of others; • When the information requested is related to a confidential investigation, litigation, or potential litigation; • When the information is diffuse and not maintained in a structured filing system; or, • Where to disclose such information would require a disproportionate effort and/or expense. Motorola must keep Personal Information accurate, complete, and up-to-date. All Data Subjects have a responsibility to assist Motorola in this effort. For further information, please contact someone in the Data Protection Office or the Law Department.	
Protection and Access to Personal Information	Motorola must employ appropriate technical and organizational security measures to safeguard Personal Information. Motorola must require agents, contractors, and other third-parties to whom Motorola discloses Personal Information in the ordinary course of its business to commit contractually to employ appropriate technical and organizational security measures that safeguard Personal Information and in so doing to refrain from any use(s) or further dissemination of such Personal Information not consistent with this Standard or not authorized in writing by Motorola. Access to Personal Information must be restricted to those employees, agents, or contractors of Motorola and its affiliates who have a legitimate business need to access that Personal Information and are authorized to do so.	MOTCS-IPS0004

	For further information, please refer to Motorola's *Information Classification and Safeguards s*tandards and the MOTCS-330 Users Must be Granted the Minimum Level of Access Required *s*tandard or contact the Data Protection Office.	
Transmission, Disclosure and Dissemination of Personal Information	Motorola must take reasonable measures to ensure that where disclosure of Personal Information is made, it is: • Done with the Data Subject's consent; • Made pursuant to an agreement; • Done as required by law or legal process; or, • Done for another lawful purpose including to advance a legitimate business activity of Motorola. Motorola employee information may be transferred for business purposes, either internally or through third parties, to countries/regions other than the country/region of origin. For further information, please contact the Data Protection Office.	MOTCS-IPS0005
Storage, Retention, and Disposal of Personal Information	Motorola must not keep Personal Information for longer than is necessary for the purpose(s) for which it was initially collected, or as required by contractual agreement, by law or regulation, by other standards, or, where applicable, for the appropriate statute of limitations period. All Motorola personnel responsible for collecting, sharing, storing or processing Personal Information must review the information periodically to determine if the information is still required to fulfill the business purpose for which it was initially collected. All Personal Information must be stored and disposed of according to Motorola's Information Classifications and Safeguards standards and Motorola's Record Management Policy. For further information, please contact the Data Protection Office.	MOTCS-463