firstonsite
Restoration

June 2011

FOS General IT Policy

FOSITGOV-001

Revision 3

FOS IT Policy

FOSITGOV-001 - IT Policy

Issued – 28 Aug 2010

Corporate IT Policy

For: **FIRSTONSITE Users**

Copies: **FILE**

i) Document Control:

Version	Revision Date	Revision Description	Author
Draft 1.0	June 12, 2008	Draft v 1	JL. Marin
Rev 1.0	Sept 11, 2008	Rev 1	JL. Marin
Rev 2.0	Aug 28, 2010	Rev 2	N. Belcher
Rev 3.0	June 1, 2011	Rev 3	N. Belcher

ii) Abstract:

This document is to be used as a Policy. This document details the Policies governing the use of computer resources and e-mail. Please refer to the Corporate IT User Policies and Standards for additional information.

iii) Table of Contents:

1)Purpose

Information Technology (IT) touches all employees, is a key enabler to the business, and helps drive business value. IT helps employees perform their jobs more efficiently and supports the achievement of corporate and departmental objectives. Information Technology has the power to improve decision-making and communications, increase efficiencies through automation of business processes, and streamline how we conduct business with customers, suppliers and other stakeholders.

As information technology becomes more advanced, integrated and increasingly present, it is important that specific technology solutions are planned, designed and deployed in a manner that optimizes outcomes for FOS, reduces total costs of ownership, and mitigates technology-related risks.

This purpose of this document is to ensure that all employees have a clear understanding of the corporate policies governing information technologies in the workplace.

Note Please read the FirstOnSite Code of Business Conduct.

2)Application of Policy

The foundation of this policy is the establishment and enforcement of enterprise IT standards, which promote cost-effective standardization and interoperability of technologies, and mitigate risks associated with technology deployments.

This policy applies to all FirstOnSite employees and authorized representatives, such as contractors and consultants (collectively, each referred to as an “employee”).

This policy is intended to set expectations and influence decisions and actions for all employees who require, acquire, develop or interact with information technologies in carrying out their roles at FirstOnSite.

This policy is intended to set expectations and influence decisions and actions for all employees who require, acquire, develop or interact with information technologies in carrying out their daily roles at FOS.

3)Scope

Includes all information technologies deployed at FOS.

Information technologies include, but are not limited to, software (business applications, process applications, operating systems, middleware, utilities, PC [personal computer] tools & applications), computer hardware (workstations/PCs, mobile devices, handheld PCs, servers, terminals, peripherals, multi-media devices), computer networks (internal/external) and devices, telecommunication systems (Cell, Phone, IP Phones, Modems, and PDA devices) and devices, document devices (printers, copiers, fax, imaging), storage, data files and data base systems.

4)Roles and Accountabilities

The Information Technology department (IT) leads information technology initiatives and is accountable for the effective deployment of information technologies at FOS.

IT is accountable for the integrity of all of FOS's corporate digital information, its business and process applications, and the security of its systems, networks, IT assets and data. IT, however, does not own corporate or departmental data. "Data ownership" resides with specific business owners who are the data custodians accountable for their data definition, use, entry and access permissions.

IT stewards the review and appropriateness of new and emerging information technologies to exploit opportunities which support the business and which are aligned with corporate goals and objectives.

IT also has a broad stewardship role to ensure that a focused and disciplined approach for systems and business process improvements occur in the planning and implementation of cross-functional business implementation initiatives.

5)Policy Statement

General

Information Technologies will be evaluated, recommended, acquired and deployed consistent with FOS's architectural technology framework and business integration models.

To achieve this, deployments must be planned, designed and developed with and through IT involvement and conform to all current published IT policies, practices and standards.

IT ensures appropriate architecture, product, technical and process standards are defined and enforced in order to promote cost-effective standardization and interoperability of technologies, and to mitigate risks associated with technology deployments.

IT both leads and stewards the review and appropriateness of new and emerging information technologies to exploit opportunities which support the business and which are aligned with corporate goals and objectives.

6)Standards

Enterprise IT standards support FOS's technology vision and strategic information technology plan. More importantly, standards promote the transformation of FOS to new enterprise solutions with reduced complexity and cost.

The establishment and governance of enterprise standards requires a constant balancing between too much and not enough control.

FOS's IT standards are intended to provide sufficient flexibility so that the business is not constrained, while simultaneously encouraging stewardship of scarce resources and promoting cost efficient ways of doing business.

7) Security

The security of FOS's data, systems, networks and IT assets is paramount.

All software and hardware deployments must be implemented with appropriate security controls and shall conform to applicable IT security standards and practices, which are developed and enforced by IT. IT involvement ensures that appropriate security controls, regulatory compliance and risk management issues are adequately addressed.

All changes to the security and control mechanisms of IT systems will be auditable.

8) Access to Corporate Electronic Information Resources

Access to corporate electronic information resources is granted to an employee based on a demonstrated need. An employee is granted only the access authority and/or system privileges necessary to accomplish assigned duties. The employee's access changes as the employee's assigned duties change and is removed when an employee no longer requires it.

Each electronic resource has a custodian who is accountable for the access to that resource.

The corporation reserves the right to deny an employee access to corporate information at any time.

All requests from outside consultants, contractors or other non-FOS personnel to access corporate electronic information resources must be coordinated through IT and approved by the appropriate FOS project coordinator and data custodian.

Violations: An employee who discovers evidence of a policy violation will immediately notify IT Security, who will initiate an investigation.

Audit: IT will conduct yearly reviews of access permissions by each custodian to verify accuracy and address inconsistencies.

Terms:

An employee is a direct employee of FOS or its subsidiaries, or a person (contractor, consultant) acting on behalf of and with the authority of FOS.

Corporate electronic information resources include data, systems, software and hardware owned by or under contract to FOS.

Corporate information is internal non-public electronic information regarding the corporation's business, assets or people.

9) Business Process Management

The successful, cost effective adoption of business systems usually requires review and reengineering of underlying business processes. In order to drive value, IT stewards the process for business process improvement and must understand the business processes embedded in IT systems and make recommendations for 'best fit' process optimization.

While the final decision on new processes belongs to the business areas, IT owns the process for designing business processes. This includes business process methodologies, tools and oversight for the business process design efforts.

As part of this mandate, IT undertakes detail process design, support for business case preparation, and change management for all major business projects with an IT component.

10) Application Software Deployment

The deployment, maintenance and support of business and process applications are the direct accountability of IT.

IT develops software architecture models, business and process integration models, standards and practices which provide guidance, based on best practices, to the design, development, implementation and commissioning of information systems.

All IT personnel will adhere to the Software Engineering Life Cycle and Change Management standards when making application software changes in a manner that ensures the integrity of all operational, regulatory and audit requirements.

All changes to the IT application software portfolio will be auditable, including traceability to the individual requesting, authorizing, validating and implementing the change.

Turnkey systems and purchased software must undergo IT technical reviews prior to acceptance and turnover to IT. IT will not support or maintain any application software that does not meet minimum IT standards.

All application software contracts must undergo IT technical review as part of the corporate process for contract management.

11) Process Control Automation

Process Control Automation will follow all IT policies and procedures detailed by the "Corporate Policies for Information Technologies." All systems used in any level of Process Control Automation must adhere to all IT policies and procedures. The IT department will steward the development process and guide the "system owners" to ensure procedures are in place to support data and system integrity, and ensure the system has a business continuity plan in place.

12) Information Technology Procurement

All information technology hardware and software procurements must conform to applicable IT standards and/or be approved by IT prior to transmittal to Purchasing. Purchasing will reject any hardware or software requests that do not meet published standards or which are not approved by IT.

Acquisition of any non-standard hardware or software requires the approval of IT management and the appropriate General Manager before transmittal to Purchasing.

All information technology acquisitions must conform to applicable IT and Purchasing practices, and FOS's corporate expenditure approvals and authority procedures.

13) Personal Computers and Handheld PCs

Personal computers, handheld PCs and similar mobile devices are corporate assets that must not only meet the business needs of the client/department, but must also comply with existing IT technical and security standards and legal requirements.

The installation of PCs and mobile computing devices, and related hardware and software, must be planned and deployed through IT. This ensures that standards compliance, on-going support, warranty administration, security administration, licensing requirements, and asset management issues are adequately addressed.

IT will publish approved hardware and software configuration options/packages for these devices that will allow employees to choose the solution that best meets their needs. IT will provide advice as required, but each department manager is accountable for reviewing the need and approving the specific configuration option.

Additional hardware or software requirements, not included in any published standard, must be accompanied by a client business justification and supported by an IT technical review.

All devices that require connectivity to FOS's network must be coordinated through IT and/or its approved vendors.

End-user 'owners' shall take reasonable precautions, particularly for mobile devices, to prevent theft, loss or breakage.

Violations: It is a violation of corporate policy to install, connect or use hardware or software that has not been deployed through or approved by IT. IT reserve the right to remove, limit, or not support or maintain software, hardware or applications that do not conform to published policies and standards.

Audit: IT will conduct blind periodic audits to ensure compliance.

14) Network

FOS's Local Area Network (LAN) and Wide Area Network (WAN) is a vital IT asset that must be rigorously managed to meet high performance standards for reliability, availability, capacity and the interoperability of devices and software systems. It provides the communications structure to support information technologies in the workplace, enabling access to, and dissemination of, corporate and process information resources.

The design of the LAN/WAN architecture and the deployment of all LAN/WAN resources is the direct accountability of IT. IT defines the network architecture and associated standards and practices which must be followed by all employees and persons acting on behalf of FOS in order to maintain the cost-effectiveness, stability and integrity of the network.

Network access is controlled through IT, and IT will not connect any device or system that does not comply with applicable standards. Wireless devices carry specific security concerns and no wireless device is to be connected unless approved in advance and registered with IT.

No personally owned equipment (PC, laptop, handheld PC, etc.) will be directly connected through any means to the LAN/WAN unless approved in advance by IT management.

No modem or remote connectivity software will be used to connect to the LAN/WAN unless approved in advance by IT management.

All new network infrastructure components will meet current FOS and industry standards, including certification, testing and documentation criteria. IT, working with other technology departments, will address deficiencies in legacy network components as part of on-going continuous improvement projects.

Terms:

The term LAN/WAN refers to FOS's internal corporate and process communications network, including all devices and media, used for data, voice and video transmission.

Network infrastructure includes all physical media used to interconnect network devices, including fiber optics, coaxial cabling, structured wiring and wireless technologies. Servers, personal computers and end-user devices are not considered 'network' infrastructure.

15) Acceptable Computer Usage

All employees and persons acting on behalf of FOS (contractors, consultants) are granted access to IT resources consistent with carrying out their assigned duties and roles. Electronic information resources are to be used solely for authorized business related activities.

All access to corporate electronic information resources is subject to corporate and IT policies, practices and applicable laws.

16) Acceptable Internet Usage

The Internet is a powerful information, research and communications tool. FOS provides Internet access for those employees who require and use it in the performance of their job and role assignments.

All employees shall comply with IT policies and practices, act in accordance with FOS's Code of Business Conduct, and follow copyright laws respecting protected software and intellectual property.

Although access to Internet resources is provided for business use, the company acknowledges that occasional personal use may occur, but this should not affect work performance or productivity.

Audit: FOS maintains the right to monitor and review Internet access and usage.

17) End User Computing

End–user clients are encouraged to develop their own personal or departmental applications using tools such as spreadsheets, data base software, or query and report generation software. Clients shall only use software approved, sourced and deployed through IT.

End-users own and maintain all personally developed applications. IT provides limited help, via the Help Desk, for various standard productivity tools that it deploys, but not for the application, data or data accuracy contained within the application. IT provides limited training on end-user tools, and specific training needs should be coordinated through the Human Resources training department.

IT provides consulting services to end-users to ensure the right tool for the application is selected and to ensure existing systems or solutions do not already exist. Some software tools have specific end-use limitations (primarily for corporate, financial, or mission-critical purposes). End-users are encouraged to consult with IT to ensure the tool and intended application is 'fit for purpose'.

Use of external software and software downloads for, or in support of, personal applications must be approved by IT and conform to appropriate IT policy, practices and legal requirements.

End-users shall store their individual or small workgroup applications on IT managed network servers to take advantage of automated backup and archiving of data and information.

18) Telecommunications

FOS provides various telecommunications services to employees in support of their normal day-to-day business activity.

Telephone and cellular phone equipment, and associated service plans, are specified and deployed through IT and its approved service provider(s).

Department managers approve all telecommunication service requests and are accountable for all charges incurred against their accountability area.

The company acknowledges that occasional personal use of telecommunication services may occur, but this should be reasonable and not affect work performance or productivity. Where long distance toll charges apply, employees are expected to reimburse the company for charges incurred.

End-user 'owners' shall take reasonable precautions, particularly for mobile devices, to prevent theft, loss or breakage.

19) Related Documents

Specific standards, practices, procedures and guidelines supporting this corporate IT Policy are continually published on IT's intranet home page as they are formally reviewed and approved. Documents that support internal IT processes may have access restrictions.

ITBOK (IT Body of Knowledge):

Our ITBOK and training documentation is available on our Intranet located at:

http://my.firstonsite.ca/training/ITBOK