GREYgroup
Famously effective since 1917

Grey Group
200 Fifth Avenue
New York, NY 10010

(212) 546-2000

Information Technology Policy

6/20/13

DOC-001

Version 1.15

Table of Contents

[redacted]

1 About This Document

1.1 Management Approval

This policy is approved by Grey senior management.

1.2 Purpose

This policy is a global policy. It establishes Information Technology requirements for users of Grey Group IT resources to ensure that Grey IT resources are properly utilized and protected from unauthorized access, abuse, fraud or loss of information. Regional offices should tailor this document to their specific circumstances. The responsibility for implementation and enforcement of this policy falls upon the regional technical director.

1.3 Scope

This policy applies to all users of Grey IT resources which includes contractors and clients as well as Grey employees.

Violations of any of the provisions of this policy are subject to disciplinary action—up to and including termination.

1.4 Review and Change of Policy

Leadership of each Grey business unit shall review and sign the **Policy Sign-off Sheet** annually. Any changes made to this document shall be noted in the **Document Revision History**.

1.5 Dissemination of Policy

Human Resources will ensure that all newly hired employees, contractors and clients who require access to Grey IT resources will review and agree to the terms of the **Information Technology Policy** and the **Acceptable Use of Information Technology Policy**.

1.6 Document Revision History

Date	Version #	Revision Summary
11/1/05	1.0	Initial draft.
11/29/05	1.1	The following changes are present in this version: **Securing Computers** section added. Users are instructed to secure their systems with a screen lock and laptops with a physical lock. **Legality of Computer Software** section added. Users are instructed to not download unlicensed software on Grey computers. **Passwords** section revised. Passwords updated every 60 days, rather than 90 days. **Change Management section.** General statement about change management. **Financial System Change Management** section revised. Added statement that

Date	Version #	Revision Summary
		new financial systems or implementation of major changes to existing system requires both GGG CIO and WPP CIO approval. **Appendix A** **Securing Computers** and **Passwords** sections have been added to the Acceptable Use policy.
12/15/05	1.2	Minor editorial changes to **Purpose** and **Dissemination of Policy** sections. Rearranged much of this document creating 2 new level 1 headings: 1. Basic Tenets 2. Applications and Operating Systems Removed **Documentation** heading. Tucked the verbiage into the **Policies and SOPs** section. Added the following verbiage to the **Purchase of Computer Software** section: All purchasing commitments shall be covered by a written purchase order and/or a supply contract which clearly states the requirements, the agreed price, the delivery or completion dates and other commercial terms as appropriate. Added section titled, **Third Party Services**. Deleted the “Acceptable Use Policy” from Appendix A. Added **Policies Control Schedule** to Appendix A and **Associated Documents** to Appendix B.
12/19/05	1.3	Minor editorial changes to **Acceptable Use**, **Legality of Computer Software**, **Antivirus Patching**, **Modems** and **Reports**. New section Data added.
1/6/06	1.4	Minor Changes to **Dissemination of Policy** and **Passwords** sections. New sections: **Email Accounts, Peer to Peer Networks** and **Connecting Personal Equipment to Grey Owned Equipment.**
8/7/06	1.5	Added the following sentence to the **Data Retention Policy** section: *This policy is in accordance with rules governing the retention of records related to the audits and reviews mandated by section 802 of the Sarbanes-Oxley Act. For more information go to the search page on the Securities and Exchange Commission website (http://sec.gov), and enter the reference code “RIN 3235-AI74.”*
9/22/06	1.6	Added “technical documentation” to the following statement: *Policies, SOPs and technical documentation shall be adjusted regularly to*

Date	Version #	Revision Summary
		accommodate changing conditions. . Policies SOPs and technical documentation shall be reviewed at least annually
4/17/07	1.7	Added the following sections: 4.3, 4.4, 4.10, 4.16, 6.2. 6.3
8/1/07	1.8	Added sections 3.1, 4.3 and 6.2
6/24/08	1.9	Slight wording changes to sections 3.2, 4.16, 5.4, 6.2 and 6.6 Revised section 5.3 to account for distinction between planned and emergency changes
8/4/08	1.10	Revised section 3.1
6/10/09	1.11	Section 1 Added "Chief of Staff" to list of approvals. Revised wording in sections 3.1, 3.5, 4.5, 4.11,5.9 and 10.1. Revised wording in section 7.3 and added the following statement: *Furthermore, any breach in security must be brought to the attention of Pete Johnston and Paul Stanley of WPP*.
7/15/09	1.12	Updated section 4.6 to conform with WPP Policy 18.4.2
2/2/10	1.13	Updated section 3.3 changed title to "Internet and Email Abuse" and added the following verbiage: *Access to the World Wide Web (WWW) and to email facilities is made available to users at Grey Group's discretion. WWW access and email are provided primarily for business purposes and not for personal use, although reasonable personal use is granted at Grey management's discretion.*
3/26/10	1.14	Moved Approval Sign-off Sheet. Added section1.1 Management Approval Updated section 2.2 to include: *Grey personnel are responsible for complying with updated terms of this policy.* Added the following sentence to Section 2.3: *Grey Group reserves the right to monitor the use of its electronic information systems including specific web sites accessed by individuals (where not prohibited by local laws)..*

Date	Version #	Revision Summary
		Added the following language to section 3.7 *All software needed to conduct business will be provided by Grey. Only authorized IT staff are permitted to copy software - from any source - onto Grey's network or computers. Grey IT users are strictly prohibited from loading any software, including games and screensavers, onto Grey's network or computers.* Removed redundant language from section 2.5
4/7/11	1.15	2.4 Legality of Computer Software Replaced LMS with "JAMF's Recon" 3.2 Securing Computers Added the following: *Workstations are configured so that a screensaver that locks the screen launches automatically after 15 minutes of inactivity.* 3.12 Modems Added "in regional offices." To following sentence. *The Grey Director of Information Security shall be informed of all modem connections in regional offices*. 3.15 Grey Network Added the following sentence: All changes affecting the Grey network must be coordinated with the Global Infrastructure Services team. 3.17 Intranets **Changed**: *All Grey intranets are subject to review by the SVP of Corporate Communications and the Grey CIO. Grey intranets include, but are not limited to, greyglobal.net. ourspace.grey.com and g.wire.* **To**: *All regional intranets are subject to review by the regional director of corporate communications and the Grey CIO.* 3.18 Peer-to-Peer Networks Requests for P2P networks must be submitted to *Director of Information Security*. Was CIO previously. 3.19 Connecting Personal Equipment Added smart phones to list of equipment 4.4 New System Implementation Process This section is new. 5.1 Purchase of Computer Hardware and Software Replaced "Grey Group" with "regional offices" in following sentence: *Wherever possible, regional offices shall make such purchases under the terms of existing agreements that WPP has with manufacturers and vendors.* 5.2 Leasing Lease agreements must be approved by regional finance director and regional technical director. Rather than Grey CFO and Grey CIO. 5.6 Third Party Services **Changed**: *All IT support contracts must be reviewed and approved by the Grey CIO, the Grey-CFO and the legal department.* **To**:

Date	Version #	Revision Summary
		All regional IT support contracts must be reviewed and approved by the regional technical director, the regional finance director and the legal department. Also changed SLA review schedule to "prior to renewal of contracts" rather than quarterly. 5.6 Electronic Trading with Third Parties Added regional technical director and regional finance director to list of approvers.
6/20/13	1.15	Added section 3.1 Secure Storage of Servers and Networking Equipment Added the following language to section 3.9 Email Accounts: *Automated processes to forward emails outside of the WPP operating group must not be used. Exceptions to this policy must be approved by either the agency's chief counsel or the WPP Director of Internal Audit.*

2 Basic Tenets

2.1 Policy Exemption

This document is a global policy with which all Grey business units must comply unless precluded by local regulations.

Requests for exemptions from any aspect of this policy must be submitted to the Grey Group CIO and then agreed to in writing by one of the following: WPP Regional CTSO's, WPP Internal Audit Director, WPP CIO.

2.2 Acceptable Use of Grey Information Technology

The **Acceptable Use of Information Technology Policy** establishes the appropriate use of Grey Group's computing and computer-based communications resources including, but not limited to, email and Internet systems. The **Grey Group Acceptable Use of Information Technology Policy** also explicitly states that information residing on the Grey network or computers is Grey (or Grey client) intellectual property. Furthermore, all software used on Grey computers shall have valid licenses and shall be installed by Grey IT. Email and Internet usage shall be monitored quarterly.

All users of Grey IT resources are required to read and accept the terms of the **Acceptable Use of Information Technology Policy** upon hire. The **Acceptable Use of Information Technology Policy** shall be distributed to Grey personnel annually. Grey personnel are responsible for complying with updated terms of this policy. Questions regarding the **Acceptable Use of Information Technology Policy** should be directed to Human Resources.

2.3 Internet and Email Abuse

Access to the World Wide Web (WWW) and to email facilities is made available to users at Grey Group's discretion. WWW access and email are provided primarily for business purposes and not for personal use, although reasonable personal use is granted at Grey management's discretion.
Use of Grey's email, Internet connection and any other information system or service, in any way that may be disruptive or offensive to others or harmful to morale is forbidden. In no case should the information systems be used to transmit messages of a sensitive, personal or private nature, or which constitute unlawful, threatening, disparaging, defamatory, scandalous or obscene material about employees, clients, vendors or any other person or entity.

For example, there is to be no display, transmission or use of email or Internet communications that contain ethnic slurs, racial epithets or anything that may be construed as harassment or disparagement of others based on their race, national origin, sex, sexual orientation, age, disability, or religious or political beliefs. The email system may not be used to solicit or proselytize others for commercial ventures, religious or political causes, outside organizations or any other non-job related solicitations. Further, there is to be no display of sexually explicit images, messages or cartoons. Grey Group reserves the right to monitor the use of its electronic information systems including specific web sites accessed by individuals (where not prohibited by local laws).

Users may make no attempts to gain access to the email of other users or to transmit messages under a coworker's credentials, except as authorized by this policy. Authorization must be provided by either the Human Resources department or the Legal department.

2.4 Legality of Computer Software

The Grey Group follows accepted industry guidelines regarding the legality of computer software. Any software installed on a Grey computer requires a valid license. Illegal use or copying of software can expose Grey management and personnel to civil and/or criminal liabilities. Grey will utilize **JAMF's Recon** software to ensure that Grey computers are in compliance with this policy.

2.5 Policies, Procedures and Operational Documentation

Policies, procedures and operational documentation shall be adjusted regularly to accommodate changing conditions. Policies procedures and operational documentation shall be reviewed at least annually or upon significant changes to the operating or business environment, to assess their adequacy and appropriateness, and amended as necessary. Management shall provide a framework and process for the periodic review and approval of standards, policies, directives and procedures. To ensure adoption of policies, management will regularly disseminate information on the nature and content of policies.

Operational documentation shall be managed accordingly:

- maintained within a version control system by the administrator of that system,

- read-only versions of technical documentation available on a share accessible to appropriate personnel

All policies shall conform to the following conventions:

- have a revision history displaying version date, version number and a revision summary;

- a title appearing on the title page and on the document footer.

3 Data/Computer Security

3.1 Secure Storage of Servers and Networking Equipment

All servers and networking equipment should be stored and operated in a physically secure environment.

3.2 Securing Physical Access to Data Centers

Access to Grey data centers is limited to authorized personnel. Authorization for data center access is governed by a separate **Data Center Access Policy**.

3.3 Securing Computers

Users are required to secure the computers that they use in their work by locking their screen whenever leaving their workstation. Workstations are configured so that a screensaver that locks the screen launches automatically after 15 minutes of inactivity. Laptop computers are to be secured physically to a desk by a lock. Local IT support should be notified if a laptop lock is needed.

3.4 Portable Computers

Laptops should be protected against loss or theft of data by use of BIOS and Hard Disk passwords where such features exist on the laptop. Consideration should also be given to securing Blackberry and similar devices.

3.5 Network Accounts

Human Resources is responsible for notifying IT of new hires, terminations and other changes to an employee's status. IT uses this information to create, delete or update the user's email and network accounts. Access to resources is governed by the principle of least privilege required.

3.6 Expiration of Non-Employee Network Accounts

Non-employee network accounts will be set to expire as follows:

- If the individual's engagement is expected to last **less than 30 days**, the network account will be set to expire on **the projected end date** of this engagement.

- If the individual's engagement is expected to last **30 days or more and this engagement starts within the first 15 days of the month**, the network account will be set to expire **at the end of the current month**.

- If the individual's engagement is expected to last **30 days or more and this engagement starts after the 15th of the month**, the network account will be set to expire **at the end of the next month**.

3.7 Passwords

All Grey IT users are responsible for taking the appropriate steps to select and secure their passwords.

All access to company networks should be password protected.

All passwords shall be changed at least every 60 days. All passwords shall conform to the standards of the system to which they provide access with regard to complexity, length and minimum duration.

Password-protected screensavers should be used on all company machines, with a maximum "wait" time of 30 minutes.

If a user needs to provide his/her password or have a new password supplied while receiving technical support, an IT technician shall force the user to create a new password, then reboot, as soon as the issue requiring support is resolved.

3.8 Data

All data and information created, stored, acquired or transmitted on company computing systems is exclusively owned by Grey (or the Client in special circumstances). All software needed to conduct business will be provided by Grey. Only authorized IT staff are permitted to copy software - from any source - onto Grey's network or computers. Grey IT users are strictly prohibited from loading any software, including games and screensavers, onto Grey's network or computers.

3.9 Email Accounts

No email mailbox shall be opened by anyone other than the owner (including IT staff) without the approval of the mailbox owner or chief counsel.

Automated processes to forward emails outside of the WPP operating group must not be used. Exceptions to this policy must be approved by either the agency's chief counsel or the WPP Director of Internal Audit.

3.10 Antivirus and Patching

All computer systems connected to the Grey Group computer network or networked resources shall have Grey Group supported and/or approved antivirus software correctly installed, configured, activated, and updated with the latest version of virus definitions. This software shall be operational at all times. At no time shall a user disable the Grey installed antivirus program. For the purposes of this policy, the network consists of systems connected to local area networks (LANs) at all of the Grey offices and subsidiaries connected by the Grey wide area network (WAN). For more details see the **Grey Group Antivirus Policy**.

All system updates shall be implemented as directed by Grey IT. Likewise, all workstations and servers are "patched" to minimize exposure to potential operating systems weaknesses. System updates shall be implemented as directed by Grey IT.

3.11 Firewalls

All Internet connections to the Grey network shall be protected from unauthorized access by appropriate firewall technology which has been approved Grey Director of Information Security.

3.12 Telecommunications Equipment and Services

The installation, replacement, upgrade or modification of telecommunications equipment or services for regional offices must be approved by the regional technical director or designee. This includes, but is not limited to: PBX's and components, mobile or cellular devices, video conference equipment, conference services, voice and data lines, etc. These commitments must be in compliance with WPP standards.

Once approved, all contracts and billing for telecommunications equipment and services will be managed by the regional office.

3.13 Modems

The Grey Director of Information Security shall be informed of all modem connections in regional offices. All modems shall have a termination date. Inbound modems must be approved by the Director of Information Security.

3.14 Wireless Security

The use of unauthorized wireless access points at any Grey Group office or partner companies is **strictly prohibited**. This policy applies to all types of wireless access points including, but not limited to, enterprise level units, small office units and personal units.

Requests for new wireless access points shall be submitted to the regional technical director of the affected office. The request should include requirements and justification.

Where wireless network cards are provided for company laptops and where laptops are provided with built-in wireless networking facilities, wireless facilities and laptops are configured with appropriate security software to ensure that unauthorized users cannot gain access to data stored on the laptop or to any company facility to which the laptop is connected.

3.15 Remote Access

Remote access to the Grey network is only provided through approved VPN entry points, using only approved VPN access devices in compliance with the **Remote Access Policy**.

3.16 Grey Network

All changes to the regional network must be approved by the Chief Technology Officer or respective Regional Technology Director Grey Director of Information Security. All changes affecting the Grey network must be coordinated with the Global Infrastructure Services team.

3.17 Internet Sites

All World Wide Web pages developed for the use of individual Grey business units must be reported to the Grey CIO. Unauthorized use, registration or set up of a domain using the Grey name must be reported to the Grey CIO. Similarly, World Wide Web pages developed by Grey for the use of WPP must be reported to the WPP CIO. Unauthorized use, registration or set up of a domain using the WPP name must be reported to the WPP CIO.

3.18 Intranets

All regional intranets are subject to review by the regional director of corporate communications and the Grey CIO. .

3.19 Peer-to-Peer Networks

The use of unauthorized “Peer-to-Peer (P2P)” networks in any Grey Group office or through Grey's network is strictly prohibited. Examples of P2P applications are Gnutella, LimeWire, Kazaa, Bit Torrent, Bug Bear, etc. All such applications are covered by this policy.

Requests for authorized use of P2P networking applications shall be submitted to the Director of Information Security. The request should include requirements and justification. IT support will assist in the deployment and use of authorized P2P applications.

3.20 Connecting Personal Equipment to Grey Owned Equipment

Personal equipment (this includes but is not limited to home laptops, smart phones connecting to email and other devices) shall not be connected in any way (this includes but is not limited to modem and Bluetooth technology) to Grey’s network or Grey owned equipment.

4 Applications and Operating Systems

4.1 WPP Approval of New Business Systems

No new business systems shall be developed, purchased or implemented without obtaining the approval of both the Grey CIO and the WPP CIO. For this purpose “business systems” includes accounting, production, timesheet and media administration systems.

4.2 IT Access to Financial Systems

IT personnel will not have functional access to financial system unless there is a written authorization by the system owner for business reason due to system limitations”.

4.3 Change Management

System changes are managed through a formal process of documentation and approvals. There are two distinct categories of change: planned and emergency.

Planned changes shall conform to the following the guidelines:

1. changes will be documented in a change control form,
2. new systems and major changes to existing systems will receive WPP approval,
3. changes will be tested,
4. appropriate approval will be obtained before the changes go into production.

Emergency changes shall conform to the following the guidelines:

1. changes will be documented in a change control form,
2. new systems and major changes to existing systems will receive WPP approval,
3. changes will be tested,
4. where time permits appropriate approval will be obtained before the changes go into production.
5. If it is not possible to obtain appropriate approval before the changes go into production, appropriate approval will be obtained as soon as possible

4.4 New System Implementation Process

The implementation process for a new system must include a proposal, a comparison of competing products/vendors, a project plan, a solution description, a solution development/configuration phase, testing, end-user training, a go-live plan that includes fallback scenarios, post implementation monitoring and analysis.

4.5 Financial Systems Change Management Policy

A change management system conforming to the specifications of the system must be in place for all financial systems used by Grey. The introduction of a new financial system and/or implementation of major changes to an existing financial system will be scheduled in accordance with WPP standards and receive the approval of the Grey CIO, the Grey Controller and the WPP CIO.

4.6 Operating System Change Management Policy

A change management system conforming to the specifications of the operating system must be in place for all operating systems used by Grey.

4.7 Data Backup and Archiving

All systems are backed up regularly. Backup frequency is determined by the system administrator in accordance with the best practices of the system. Backup tapes are stored off-site at a professional data storage facility. Data requirements for off-site storage are determined by individual Grey business units.

4.8 Data Restoration

Data restoration is carried out in accordance with the best practices of the system being restored.

4.9 Data Retention Policy

All data is backed up and stored in compliance with local legislative requirements. This policy is in accordance with rules governing the retention of records related to the audits and reviews mandated by section 802 of the Sarbanes-Oxley Act. For more information go to the search page on the Securities and Exchange Commission website (http://sec.gov), and enter the reference code "RIN 3235-AI74."

4.10 Disaster Recovery

All Grey Group offices must have a current disaster recovery plan. Each office must review, test and update their disaster recovery plan annually.

5 IT Resource Procurement

5.1 Purchase of Computer Software and Hardware

All purchasing commitments shall be covered by a written purchase order and/or a supply contract which clearly states the requirements, the agreed price, the delivery or completion dates and other commercial terms as appropriate. All purchases of computer software and/or hardware require Finance and IT approval. Wherever possible, regional offices shall make such purchases under the terms of existing agreements that WPP has with manufacturers and vendors. Purchases outside of WPP agreements must be approved by the WPP CIO.

5.2 Leasing

IT equipment or services must not be acquired under operating or finance leases or rental agreements without the prior approval of both the regional finance director and the regional technical director.

5.3 IT Purchases Exceeding $25,000

All purchases of IT equipment or services in excess of $25,000 require the approval of the Grey CIO.

5.4 Purchase of Business Applications

The purchase of any workflow, production, asset management or business related application must be approved by the Grey CIO.

5.5 Internet Sites and Software Developed for Clients

The intellectual property rights in any software developed for client use by Grey and provided as a service or product to a client shall be protected.

Appropriate legally binding terms and conditions must accompany all software provided to clients such that the company's risks are mitigated.

The provision of any software, hardware or services to clients should be covered by a written agreement, which has been reviewed by company lawyers and signed by all affected parties. Risks covered by such an agreement would include, but not be limited to:

- maintenance of internal intellectual property;
- other copyright issues;
- fitness for purpose (warranties should be avoided);
- support and maintenance procedures.

5.6 Third Party Services

All regional IT support contracts must be reviewed and approved by the regional technical director, the regional finance director and the legal department. Any existing Service Level Agreements with vendors will be reviewed prior to renewal of contracts.

5.7 Electronic Trading with Third Parties

All agreements for electronic trading with third parties shall be approved by the regional technical director, the regional finance director, the Grey CIO and the Grey-Finance.

6 Enforcement

6.1 Monitoring

To monitor compliance with the Grey IT Policy see the **Policy Controls Schedule** in Appendix A.

6.2 Reports

At the conclusion of an IT audit, the department responsible for conducting the audit must submit a report to the Grey CIO detailing the results. The results of the IT Audit will be reported to the Finance Director and discussed during the Monthly Meetings.

6.3 Escalation Procedure

Instances of non-compliance within a Grey business unit are to be brought to the attention of the appropriate IT Director, HR manager and Finance Director of that business unit. Furthermore, any breach in security must be brought to the attention of the WPP CISO and WPP Head of Audit.

[redacted]

7 Appendix A

7.1 Policy Controls Schedule

Check	Audit Frequency	Responsible Department
Distribution of **Acceptable Use Policy**.	Annually	Information Technology/ Human Resources
Data center access. Review list of all authorized data center users	Monthly	Information Technology/ Finance
Regularly scheduled password changes.	Monthly	Information Technology
System Performance Report	Monthly	Information Technology
Antivirus and patches are current.	Monthly	Information Technology
Backup admin reviews previous night's backup jobs and re-runs failed jobs. Recurring backup failures are reported to management	Daily	Information Technology
Disaster recovery plan for work locations.	Annually	Information Technology
Documentation is current and accurate	Annually	Information Technology
Firewalls rules review.	Quarterly	Information Technology
Wireless access connections and hardware are secure.	Quarterly	Information Technology
Remote access is only available to authorized users.	Monthly	Information Technology

8 Appendix B

8.1 Additional Policies

Additional IT policies are listed below

Document File Name	Description
Acceptable Use of Information Technology Policy	Establishes guidelines for proper use of Grey IT resources.
Data Center Access Policy	Establishes guidelines for how entry to the data center is monitored
Data Backup Policy	Detailed data backup policy.
System Monitoring and Reporting Policy	Identifies what monitoring packages are used on particular servers and downtime thresholds.
Remote Access Policy	Establishes guidelines for obtaining and using the remote access privileges.
Antivirus Policy	Policy provides framework for defense from and remediation of virus outbreak.
Wireless Policy	Policy addresses both deployment of wireless access points as well as configuration of wireless enabled laptops.
Firewall Policy	Provides guidance that defines the overall firewall strategy for Grey Global Group.
Asset Management Policy	Establishes guidelines for the management of information technology assets.

9 Appendix C Information Technology Policy Employee Agreement

I have received, read, understand and agree with the
Information Technology Policy.

Company: ________________________

Title: ________________________

Print Name:________________________

Signature:_________________________ **Date**:___________

10 Appendix D Management Policy Approvals

Leadership of each Grey region is required to provide signed approval of this policy annually.
The regional IT director shall secure these signatures and retain the signed document as evidence of approval.

Name/Position	Signature	Date
James Heekin CEO		
Robert Walsh CIO		7/10/13
Robert Oates CFO		
John Grudzina COS		