**THE SCOTTS MIRACLE-GRO COMPANY & SUBSIDIARIES**

**CORPORATE POLICY W-AA-7** **USE OF SCOTTS INFORMATION SYSTEMS**

**To:** All Associates Date: July 1, 2003

Revised: October 1, 2008

**From:** Vincent C. Brockman, Executive Vice President and General Counsel

## GENERAL POLICY

It is the policy of The Scotts Miracle-Gro Company (the "Company") that the telephone, facsimile, computer and communications systems (collectively, the "Information Systems") of the Company be used solely for the benefit of the Company. Information Systems provided by the Company are Company property, and their purpose is to facilitate and support Company business. All users have the responsibility to use these resources in a professional, ethical and lawful manner. Information Systems subject to this Policy include, but are not limited to, all desktop, laptop and other computers and computer networks including the Company's Intranet and Internet access means, providers and systems, the electronic mail system ("e-mail"), the telephone system, voice mail system, all company-provided cellular phones, Blackberries and other PDAs, and the fax system of the Company.

Information Systems should not be used in any way which violates any other Company Policy, such as the Company Policy on sexual harassment.

All files, e-mail messages, Blackberry or other PDA messages, telephone conversations if recorded, voice mail messages, Internet usage information (including content and data uploaded to the Internet, navigational information and history, as well as cookie and cache files), documents and other records which are created or transmitted using or which are received or stored on the Information Systems are the property of the Company and may be accessed, intercepted, reviewed or listened to, copied, deleted, and/or disclosed at any time by the Company, with or without notice, when it deems it appropriate to do so in its sole judgment.

Intentional and unjustified accessing, intercepting, reviewing, or copying of files, e-mail messages, voice mail messages, documents and other records of other persons which are created or transmitted using or which are stored on the Information Systems, is prohibited. The Company reserves the right to review any and all Associate files that are part of the Information Systems to ensure compliance with the law, this Policy and any other Company policy.

## SPECIFIC GUIDANCE

1. The Information Systems are intended to be used for company business and are not intended for personal use. The Company recognizes that incidental and occasional use of Information Systems for personal purposes is inevitable, but this use must not interfere with the Company's use of the Information Systems, and in any event will always be subject to scrutiny and possible disapproval by the Company. The Company will be the sole judge of whether any particular personal use complies with this Policy.

2. While this Specific Guidance is intended to provide Company Associates with information regarding use of the Company's Information Systems, it is not exhaustive, and the Company reserves the right to add additional requirements or restrictions.
3. The Company possesses and may utilize the technology to digitally record all telephone calls. The primary purpose of this technology is (i) to provide the Company's Consumer Service department with the ability to record consumer calls for training, evaluation or other purposes; and (ii) for review and evaluation of threats to the security or safety of the Company or its Associates. Digitally recorded telephone calls not related to the Consumer Service department may be reviewed from time to time but only with the approval of the Company's senior legal and human resources executives and, where appropriate, its chief executive officers.
4. Individuals should not expect privacy for any files, messages or materials created or transmitted using or stored on the Information Systems (even though security may be placed on a document or file and regardless of whether passwords are employed), or for any access to the Internet made through Information Systems. This is true regardless of whether a file, e-mail message, voice mail message, document or other record or Internet access is related to personal or to business use. By using the Information Systems to send or receive messages, to author or store files or documents, or to access the Internet, an associate consents to the Company's accessing, intercepting, reviewing, listening to, copying, deleting, and/or disclosing any such message, file, document or Internet access, with or without notice, when the Company deems it appropriate to do so in its sole judgment. The Company reserves the right to review any and all of the files and Information Systems used by Associates to ensure compliance with all laws, this Policy and any other Company policies. Associates should not assume communications using Information Systems are private, and if they have sensitive information to transmit, they should use other means.
5. Information Systems and services should not be used in a manner that is likely to cause computer network congestion or significantly hamper the ability of other people to access and use the Information Systems.
6. To prevent computer viruses from being transmitted through the Company's computer system, unauthorized downloading of any unauthorized software is strictly prohibited. Associates should contact the Global Business Information Services ("GBIS") administrator if they have any questions.
7. Every associate is responsible for the protection of the Company's proprietary and/or confidential information. Accordingly, under no circumstances will information of a confidential, sensitive or otherwise proprietary nature be placed or posted on the Internet or transmitted outside of the Company via e-mail, voice mail or otherwise be disclosed to anyone outside the Company without prior written management approval.
8. No media advertisement, Internet home page, electronic bulletin board posting, electronic mail message, voice mail message or any other public representation about the Company or on behalf of the Company may be issued unless it has first been approved by a Department Manager, and Corporate Communications or other appropriate management.
9. Any use of the Company's name or service marks outside the course of the user's employment without the express written authorization of Company management is prohibited.
10. Associates may not access e-mail, the Internet, voice mail or the Company's computer system using another employee's password or personal identification. "Spoofing," constructing electronic communications so it appears to be from someone else, is also prohibited.
11. Associates may not take any action designed to hide the fact that they are using the Company's computer system, e-mail or the Internet. The user name, electronic mail address, organizational affiliation, time and date of transmission, and related information included with electronic

messages or postings must always reflect the true originator, time, date, and place of origination of the messages or postings as well as the true content of the original message.

12. The e-mail system is not to be used in ways that are disruptive, defamatory or offensive to others, or in ways that are inconsistent with the professional image of the Company or are prohibited by law.
13. Display or transmission of sexually explicit images, messages, cartoons or any communication that can be construed as harassment or disparagement of others based on their race, national origin, sex, age, disability, or other protected class is prohibited. This includes, but is not limited to, a specific prohibition on using the Information Systems to view or store images of pornography. Associates are advised that viewing and/or storing images of child pornography may violate federal law and that the Company may report such activities to the appropriate authorities.
14. Associates may not distribute copyrighted material (i.e. computer software, screen savers, articles, graphics files, etc.) via e-mail, the Internet or the Company's computer system without confirming that the Company has a right to copy and distribute the copyrighted material. If you have any questions about whether the Company has a right to distribute copyrighted material, please contact the office of the General Counsel.
15. Information Systems will not be used to solicit on behalf of outside business ventures or address others regarding commercial, religious, charitable or political causes or for any other solicitations that are not work related except as approved by management in writing.
16. Any employee who violates this Policy may be subject to disciplinary action, up to and including termination.
17. Associates must be familiar and comply with the provisions of Policy W-GS-9, Handheld Wireless Device Policy, including but not limited to the safety provisions relating to use of a cell phone and those prohibiting response to BlackBerry, PDA or text messages while driving.
18. The provisions of this Policy are applicable even if associates are accessing the Company's Intranet or other components of the Information Systems from remote locations such as home or non-company computers.
19. REFERENCES - Other Corporate policies (published on the Scotts Intranet) containing additional related guidance that associates should be familiar with include, but are not limited to:

    a. Corporate Policy W-AA-1 CODE OF BUSINESS CONDUCT AND ETHICS
    b. Corporate Policy W-FN-1 INTERNAL CONTROLS
    c. Corporate Policy W-AA-3 CONFIDENTIALITY OF COMPANY INFORMATION
    d. Corporate Policy W-IS-1 INFORMATION SERVICES
    e. Corporate Policy N-HR-4 ANTI-HARRASSMENT POLICY
    f. Corporate Policy W-GS-9 HANDHELD WIRELESS DEVICE POLICY