

Protecting Our Information Assets is Everyone's Responsibility

Information Assets are a vital part of the success of the business of the Company. Yet never before have Information Assets been so vulnerable to loss. Each year, businesses report the loss of billions of dollars due to theft of proprietary electronic information, financial fraud, or sabotage of critical electronic data.

Our Information Assets are a critical part of our success and protecting them is a top priority. Therefore, a new era of information security has begun at Sims Metal Management. The implementation of the policies set out in this document is a cornerstone of that new era. Please carefully read this entire Information Security Policy ("Policy") and together we may better protect our business.

About this Policy

This Policy sets out the Company's policies in relation to:

- (i) information security,
- (ii) the Company's Email System, and
- (iii) the Company's Internet systems.

This Policy applies to all of the Company's Employees and all Employees must comply with this Policy at all times.

Please note that this Policy is not the only Company policy related to the security of our Information Assets. Please also review the Company Code of Conduct (available at our website, www.simsmm.com), specifically sections 3.15, 3.17, and 3.18, as well as your region's Employee handbook, and other pertinent policies as they are distributed from time-to-time. In the event that any Company policy appears to conflict or be inconsistent with this Policy, the order of priority for controlling policies is: the Code of Conduct ("the Code"), this Policy, related global Company policies, regional Employee handbooks, and related regional policies. Capitalized terms in this Policy document are as defined herein (please refer to "Definitions" section below). This dated Policy supersedes all prior versions of this Policy and all other Company policies relating to the Company's information security, Email System and Internet system, except as stated above.

Employees who fail to comply with this Policy may be subject to disciplinary action, including suspension or restriction of Information Resources usage rights and dismissal in sufficiently serious circumstances, in accordance with the Code, the applicable Employee handbook, this Policy and other applicable policies. In addition, conduct that is unlawful under Applicable Laws may mean individual Employees could face civil, and in some cases criminal, liability. Use of any Company Information Resources for illegal activity is grounds for immediate dismissal, and the Company will cooperate with any legitimate law enforcement activity with respect to any such alleged activity.

A. Purpose of Information Security Policy

Sims Metal Management protects its Information Assets to ensure:

- (a) the confidentiality of Company Confidential Information,
- (b) privacy of personal information (in accordance with law),
- (c) integrity and availability of Information Assets when needed for Company purposes,
- (d) prevention of inappropriate use of or unauthorized access to Information Assets,
- (e) compliance with law,
- (f) the security of all Information Resources, and
- (g) control of applicable operating costs.

The purpose of this Policy is to set forth the Company's expectations of its Employees and requirements regarding the protection of its Information Assets and use of the Internet and Email System, and to clarify responsibility for ensuring those expectations and requirements are being met, as well as to clarify that there should be no expectation of privacy with respect to communication by means of Information Resources.

B. Definitions

Access Manager means, in reference to an Information Asset, the Information Technology Department Employee directly responsible for implementing any controls on access to that Information Asset, or class of Information Asset. Decisions regarding appropriate controls on any specific Information Asset or class of Information Asset may be made, if otherwise in accordance with this Policy, by senior Company or regional management or in appropriate instances, as set out in this Policy, by the Director of Information Technology either directly or as appropriately delegated.

Applicable Laws means all laws and regulations applicable to the Company in a jurisdiction where the Company or the relevant Company affiliate operates.

Company or Sims Metal Management means Sims Metal Management Limited and each of its majority owned or otherwise controlled affiliates.

Confidential Information means all confidential, sensitive, and proprietary business information, ideas, data, and trade secrets of the Company, and includes all information subject to:

- (a) the Confidentiality provision of Section 3.17 of the Code,
- (b) any confidentiality agreement with any third party,
- (c) any privacy or confidentiality requirement in accordance with contract or law,
- (d) any confidentiality provision of any Company Employee handbook, and
- (e) any other confidentiality restriction in accordance with the business needs of the Company.

Confidential Information includes, but is not limited to, Company owned, developed, leased, or licensed: computer programs and other computer systems information; and computer software algorithms.

Employee means a director, officer or Employee of the Company.

Information Asset means any (a) electronically stored or generated Confidential Information and/or (b) any Information Resources.

Information Resources means any computer hardware (e.g. desktops, laptops, PDAs) or software (including applications software and operating systems) owned, developed, leased, or licensed by the Company, storage media (e.g. CD-ROMS, DVDs, hard disks, floppy disks, memory devices), networks, email and Internet facilities used by the Company (or any part of it).

Information Security Standards means the documented requirements identified by the Director of Information Technology for the purpose of achieving the objectives of this Policy, and from which the information security components of Company procedures are derived.

Information Technology Department means the Company's department responsible for the Information Resources.

IT Steering Committee means a group comprised of representatives of each business unit of the Company, appointed by the head of such business unit, charged with responsibility for assisting the Director of Information Technology in the performance of the duties set forth in this Policy.

Director or Director of Information Technology means the **Information Technology Department** Employee of the Company charged with primary responsibility for maintaining, amending, and implementing this Policy.

C. Information Assets Security Requirements

1. Controlled Access.

Only designated Access Managers are authorized to provide Employee access to Information Resources, in accordance with established Company approval procedures; however such Access Manager or the Director or his/her designee may provide means for use of classes of Information Resources without need for specific authorized access for each such Information Resource. For example, either the Director or the applicable Access Manager may authorize the downloading of a certain class of software such as the current version of Adobe Acrobat®

If more than one business unit requires access to an Information Resource, those units shall coordinate their efforts with the appropriate Access Manager. Any unresolved issues regarding such access may be referred to the Director, and if they remain unresolved, to the IT Steering Committee.

For access to certain Information Resources, the Access Managers must assign each authorized user a unique identification code (user ID) and must use passwords or other authentication methods to control access to such Information Resources and related Information Assets. Users must not share unique user IDs or passwords.

2. External Relationships.

To the extent that access to Information Assets is granted to or Information Assets are shared with third parties such as lawyers, accountants, insurance brokers, consultants, contractors, vendors, and business partners, those third parties must agree by written contract to:

- (a) adhere to the requirements of this Policy (whether by specific reference to the Policy or otherwise), or
- (b) to otherwise protect the Information Assets in a manner equivalent to and consistent with this Policy.

Third parties must only be permitted to access Information Assets to the extent required to permit them to perform their responsibilities to the Company.

In addition, transfers of certain Information Assets to third parties by any electronic medium (e.g. tape, FTP file transfer) also require an approved corporate data release, either by means of contract or otherwise. Such Information Assets would include but are not limited to personnel data subject to privacy requirements under Applicable Laws. It is understood however that certain Information Assets regularly are shared by e-mail between the Company and third parties in the ordinary course of business. It is not the intent of this Policy to interfere with the exchange of such Information Assets, provided that such exchange is not inconsistent with the Code, this Policy or the Company's other protections of Confidential Information.

If access to the Company computer network is required by a third party, it may only be provided upon authorization by the Director, his/her designee, or the appropriate Access Manager, who will be responsible for confirming whether the third party's information security measures are consistent with this Policy, to the extent appropriate for the class of such Information Asset and the risk posed by the third party gaining access to it. Such confirmation may include, where appropriate: on-site inspections; computer system monitoring; reviewing third party documentation; reviewing internal or external audit results; obtaining summaries of test results or the equivalent; evaluation of contract terms or other reasonable means to ensure delivery of audit, test and other documentation regarding the third party's information security measures; and reviewing appropriate reports on the third party's security measures. Any reports or audits should be prepared in accordance with Applicable Laws, for example in the United States this may include preparation in accordance with the AICPA Statement of Auditing Standards No. 70, "Reports on the Processing of Transactions by Service Organizations" (SAS 70).

3. Personal Use of Information Assets.

Personal use of Information Assets must be consistent with the Code, the applicable Employee handbook, and this Policy. Employees are not permitted to:

- a) use Information Assets for unauthorized or personal purposes or gain; or
- b) allow third party use of Information Assets for unauthorized or personal purposes or gain.

Notwithstanding the above, in accordance with the Code, with respect to Information Resources, modest personal use may be allowed if unrelated to outside business activities and if it does not interfere with Company business or the performance of Company duties.

4. Hardware and Software Configurations.

All Information Resources must be configured and protected by security measures in accordance with Company requirements and Applicable Laws. Such measures may include encryption of data on mobile devices where required by Applicable Laws. Subject to the above, the Director or designee or appropriate Access Manager must approve any changes to the configuration, location, or installation of applicable new software and/or hardware. No personal equipment may be connected to the Information Resources without such approval, and any personal equipment used in connection with the Information Resources must be equipped with approved security measures, for example anti-virus software.

5. Backup and Recovery.

Access Managers must ensure that, where applicable, Information Assets are regularly backed up and adequate measures are in place to ensure that they are recoverable in the event they are lost, damaged or altered.

6. Physical Security.

Facilities in which Information Assets are maintained are to be kept secure from unauthorized access. Employees must comply with all security procedures set by the Company from time to time.

7. Electronic Discovery.

The requirements in this Policy are subject to any mandatory requirements of Applicable Laws, including requirements under Applicable Laws related to the disclosure of electronic information that may arise in the course of litigation proceedings.

8. Ownership.

All Information Assets whether related to business or personal usage of Information Resources are and always remain Company property.

9. Amendment.

The Company reserves the right to amend this Policy at any time and will issue or make available revised versions to relevant Employees.

D. Information Security Policy Compliance Requirements

1. Director of Information Technology.

The Director is responsible for:

- (i) maintaining, implementing, and amending this Policy;
- (ii) publishing and maintaining appropriate Information Security Standards upon approval of the IT Steering Committee; and
- (iii) ensuring compliance with Applicable Laws, such as data privacy requirements, in relation to the Information Assets.

The Director of Information Technology may delegate any of these responsibilities to appropriate Company personnel.

2. Monitoring.

The Access Manager for each applicable Information Asset or class of Information Asset must ensure that:

- (i) the use of that Information Asset or class of Information Asset is adequately monitored; and
- (ii) computer system logs are maintained and reviewed for compliance with this Policy and other applicable Company policies and Information Security Standards.

The Director must ensure that the Access Managers review, approve, update and keep up-to-date a list of Employees and other persons who are authorized to have access to the relevant Information Assets or classes of Information Assets as and when required and at least annually.

3. Risk Assessments.

The Director, in coordination with other designated Employees, is responsible for:

- (i) identifying reasonably foreseeable internal and external security threats to Information Assets that could result in unauthorized disclosure, misuse, alterations or destruction of Information Assets;
- (ii) assessing the likelihood and potential damage of those threats taking into consideration the sensitivity of the relevant Information Assets;
- (iii) assessing the sufficiency of Information Resources, policies, procedures, third party information systems and other arrangements in place to control such risks; and
- (iv) ensuring that all identified security deficiencies are addressed as soon as possible.

4. Violations.

Employees who fail to comply with this Policy may be subject to disciplinary action by the Company and other consequences, as set out at the start of this Policy.

5. Reporting.

Employees must immediately report any suspected security incidents in relation to the Information Resources or breaches of this Policy or the Company's Information Security Standards to their immediate supervisor, the next level of management, or the appropriate Access Manager, or other appropriate personnel, such as the Director, in accordance with the Code, the applicable Employee handbook, and this Policy, or otherwise to the Company via the Sims Metal Management Ethics & Compliance Hotline (as outlined in the Code).

6. Compliance Acknowledgement.

Employees are required to confirm their understanding and agreement to comply with this Policy and all published Information Security Standards by signing an Information Security Policy Acknowledgement form as and when requested by the Company. New Employees are also required to do so when they join the Company. The Company's applicable regional Human Resources Department will be responsible for obtaining and maintaining signed copies of these Acknowledgements.

E. Email Policy

The Company maintains an electronic mail system ("Email System"). The Email System is provided by the Company to assist in the conduct of Company business. The Company has established policies and conditions with respect to use of the Email System (both on Company premises and via mobile devices) and the usage, disclosure, monitoring, and distribution of e-mail created, sent, and received by means of Company Information Resources. Those policies and conditions are set out in the Code, applicable Employee handbooks, and in this Email Policy. Employees must comply with the following conditions in relation to use of the Company's Email System:

1. The Email System is Company property. All messages composed, sent, or received on the Email System (including any intellectual property rights in such messages) are and remain the property of the Company. They are not the private property of any Employee.
2. The use of the Company Email System is intended for the conduct of Company business, except that modest personal use may be allowed provided such use is consistent with the Code, applicable Employee handbooks, and this Policy, and with the extent to which the Company allows use of Company telephones for personal telephone calls. If in any doubt Employees should check with their manager as to the level of personal use that is regarded as acceptable. The Company Email System may not be used for any purposes which are not permitted for Information Assets, including personal business activities, such as in relation to commercial ventures, religious or political causes, or outside organizations. The Company maintains the right to withdraw authorization of all or just private use of the Email System, at the Company's sole discretion, for individual Employees or groups of Employees without notice.
3. No Employee may use the Email System to create or transmit any messages that are defamatory or otherwise offensive to others, disruptive of Company business or otherwise in violation of Applicable Laws or any Company policy. Among those messages which the Company deems offensive are those messages inconsistent with Company harassment, non-discrimination, or anti-violence policies set out in the Code or in applicable Employee handbooks, including those messages which contain sexual suggestions, racial slurs, gender offensive comments, or any other comment that may offend someone's status as a member of a particular group which is protected by anti-discrimination legislation under Applicable Laws.
4. Employees must not use the Email System in connection with any of the prohibited activities or materials referred to in the Internet Usage Policy below.
5. The Email System shall not be used to send (upload) or receive (download) non-Company copyrighted materials, trade secrets, proprietary financial information, or similar materials without appropriate prior authorization, except to the extent allowed by Applicable Laws.
6. The Company reserves the right to monitor and access all messages created, received or sent over the Email System to the extent permitted by Applicable Laws. For example, this may include investigating compliance with Company policies, protecting other Company personnel, or maintaining security of the Computer Systems. The contents of email properly obtained for legitimate business purposes may be disclosed within the Company without permission of the Employee who created, received or sent the relevant electronic mail, in accordance with Applicable Laws.
7. Please be aware that the confidentiality of any message on the Email System cannot always be guaranteed and Employees must take appropriate care regarding messages of a confidential nature. Even when a message is erased, it is still possible to retrieve and read that message. Further, the use of passwords for security does not always guarantee confidentiality.
8. Email messages should be treated as confidential and accessed only by the intended recipient. Except as otherwise specifically provided for herein, Employees are not authorized to retrieve or read any email messages that are not sent to them unless part of their normal duties (for example, by a secretary for their manager and as authorized by

their manager). Any exception to this must receive prior approval by an appropriate member of the Company's management.

9. Employees must only use the email identification and passwords assigned or selected by them in relation to the Email System in accordance with procedures approved by the Director (or as delegated). No Employee may use another Employee's identification and passwords unless specifically approved by the Director (or as delegated).
10. All messages sent using the Company Email System must use whichever disclaimer is deemed appropriate for such use as set at the discretion of the Company from time-to-time in accordance with Applicable Laws, such as any disclaimer for which the Director or delegate provides subsequent policy requirements (whether added automatically by the applicable Company server or required to be added manually).
11. Emails are a permanent form of communication that can be used as evidence in legal proceedings. Therefore Employees must take the same level of care when writing emails as would be appropriate for a formal business letter.
12. All messages sent using the Company Email System and email logs must be treated in accordance with Applicable Laws and the applicable Company retention or destruction policy as set at the discretion of the Company from time-to-time, such as any policy set by the Director or regional delegate.
13. Payment or reimbursement by the Company of email-related expenses incurred by Employees other than in accordance with this and other applicable Company policy is prohibited.
14. Employees should immediately report any suspected violations of this Policy to their immediate supervisor, the next level of management, or the appropriate Access Manager, or other appropriate personnel, such as the Director, in accordance with the Code, the applicable Employee handbook, and this Policy, or otherwise to the Company via the Sims Metal Management Ethics & Compliance Hotline (as outlined in the Code).
15. Employees who fail to comply with this Policy may be subject to disciplinary action by the Company and other consequences, as set out at the start of this Policy.
16. The Company reserves the right to amend this Email Policy at any time and will issue or make available revised versions to relevant Employees.

F. Internet Usage Policy

The Company provides certain Employees with access to the vast information resources of the Internet to help those Employees perform their job faster and smarter and be well-informed on issues of concern to the business of the Company.

The Information Resources to provide that access to the Internet represent a considerable commitment of Company resources for telecommunications, networking, software, and electronic data storage. This Internet Usage Policy is designed to help those Employees able to access the Internet using Company Information Resources to understand the expectations of the Company for the use of those resources in the particular context of the Internet, and to help those Employees use those resources wisely.

INFORMATION SECURITY POLICY

The Company has established policies with respect to the usage and monitoring of Internet activity by means of Company Information Resources. Those policies are set out in the Code, applicable Employee handbooks, and in this Internet Usage Policy. Employees must comply with the following conditions in relation to use of the Company's Internet systems:

1. The use of the Company's Internet Information Resources is intended for Company-related business including research, communication, and professional development within the broad business objectives of the Company, except that modest personal use may be allowed provided such use is consistent with the Code, applicable Employee handbooks, and this Policy, and with the extent to which the Company allows use of Company telephones for personal telephone calls. If in any doubt Employees should check with their manager as to the level of personal use that is regarded as acceptable. Company Internet Information Resources may not be used for any purposes which are not permitted for Information Assets, including personal business activities, such as in relation to commercial ventures, religious or political causes, or outside organizations. The Company maintains the right to withdraw authorization of all or just private use of Company Internet Information Resources, at the Company's sole discretion, for individual Employees or groups of Employees without notice.
2. The Company has software and systems in place to monitor and record all Internet usage by means of Information Resources. Company security systems are capable of recording (for each and every user) each World Wide Web site visited, each chat, newsgroup, and each file transfer into and out of our internal networks. The Company reserves the right to monitor or record any or all Internet usage by means of Information Resources at any time in accordance with Applicable Laws. No Employee should have any expectation of privacy as to his or her Internet usage by means of Information Resources, except to the extent that privacy is permitted under Applicable Laws. Company managers may review Internet activity by means of Information Resources and analyze usage patterns. They may choose to publicize this data for any legitimate business purpose such as to ensure that Company Internet resources are devoted to maintaining the highest levels of Employee and Information Resource productivity.
3. Employees should not assume that any electronic message sent or received using Company Internet-related Information Resources is confidential and Employees must take appropriate care regarding messages of a confidential nature. Even when such a message is erased, it is still possible to retrieve and read that message.
4. Personal use of Internet services by means of Information Resources should not interfere with Company business operations and normally should be limited to non-working hours (e.g. breaks, lunch). If in any doubt Employees should check with their manager as to the level of personal use that is regarded as acceptable.
5. No Employee may use the Company's Internet system, or any other Information Resources (e.g. network or computer resources) to view, archive, store, distribute, edit, record, or copy anything that is defamatory or otherwise offensive to others or disruptive of Company business or otherwise in violation of Applicable Laws or any Company policy. Such material includes but is not limited to material which is inconsistent with Company harassment, non-discrimination, or anti-violence policies set out in the Code or in applicable Employee handbooks, including any material which contains or depicts sexual suggestions, racial slurs, gender offensive comments, or any other comment or depiction that may offend someone's status as a member of a particular group which is protected by anti-discrimination legislation under Applicable Laws.

6. The Internet shall not be used to send (upload) or receive (download) non-Company copyrighted materials, trade secrets, proprietary financial information, or similar materials without appropriate prior authorization, except to the extent permitted by Applicable Law.
7. The Company has no control over the information or content accessed through the Internet, except to the extent that it implements applicable filters. The Company cannot be held responsible for information or content accessed through the Internet.
8. Except as otherwise provided for herein, use of Internet systems by means of Information Resources or personal devices to receive (download) software programs, utilities or software extensions is prohibited without prior authorization from the Director or his/her delegate or the Access Manager. This includes (but is not limited to) screen savers, games, and utility programs. Loading any such software onto personal devices or onto the Information Resources from any other media (e.g. memory device, CD-ROM) is prohibited without prior authorization from the Director of Information Technology.
9. Any software or files downloaded via the Internet into Information Resources become the property of the Company. Any such files or software may be used only in ways that are consistent with their licenses or copyrights.
10. No Employee may use Company Information Resources knowingly to download or distribute pirated software or data. The use of file swapping software on Company Information Resources is prohibited.
11. No Employee may use the Company's Internet system or any other Information Resources to deliberately or negligently propagate any virus, worm, Trojan horse, trap-door program code, or any other software designed to cause harm.
12. No Employee may use the Company's Internet system or any other Information Resources to knowingly disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.
13. No Employee may knowingly use this Company's Internet system or any other Information Resources to infringe any intellectual property rights or Applicable Laws.
14. Each Employee using the Internet by means of Information Resources for Company business shall identify himself or herself honestly, accurately and completely (including his/her group company and job title where requested) when participating in chats, newsgroups, instant messaging sessions, text messages or similar Internet communications or when setting up accounts on outside computer systems. Employees may only do so in the proper course of their work and in accordance with paragraph 17 below. If in any doubt as to whether this is allowed, an Employee must check with his/her manager.
15. Employees who use chats, newsgroups, instant messages, text messages, e-mail or similar Internet communications must take special care to protect the clarity, consistency and integrity of the Company's reputation and must comply with paragraph 17 below. Anything any Employee communicates through the Internet in the course of working for the Company may be taken as representing the Company's views. For this reason, users of the Company's Email System are prohibited from using their Company-provided e-mail address (e.g. someone@simsmm.com) or otherwise identifying themselves as Employees of the Company when participating in non-work related online discussion

INFORMATION SECURITY POLICY

forums, bulletin boards, web sites, chat sessions, instant messaging sessions, or text messages.

16. Temporary or contract workers are not permitted to use the Company's Email System or Internet system unless authorized by the Director, his/her delegates, or an appropriate manager.
17. Only those Employees or other Company representatives who are specifically and expressly authorized to speak to the media, to analysts or in public gatherings on behalf of the Company, in accordance with applicable Company policy, may speak/write in the name of the Company to any newsgroup, chat room, instant messaging sessions, text message or other method of electronic communication. Other Employees may participate in newsgroups, chats, instant messages, or text messages in the course of business when relevant to their Company duties, but they must make clear that they do not do so on behalf of the Company and must not disclose any Confidential Information without authorization. Where an individual participant is identified as an Employee of this Company, unless properly authorized to do so the Employee must refrain from giving any political views and from endorsing or appearing to endorse on behalf of the Company any commercial product or service not sold or serviced by this Company. Only those Company officers and representatives who are authorized to speak to the media, to analysts, or in public gatherings on behalf of the Company, in accordance with applicable Company policy, may grant such authority to participants in newsgroups, chat rooms or other Internet communications.
18. Employees are reminded that chats, newsgroups, instant messages, text messages and other Internet communications can be public forums where it is inappropriate to reveal Confidential Information of the Company (such as customer data, trade secrets, and any other material covered by existing Company Confidential Information policies).
19. The Company retains the copyright to and all other intellectual property rights in any Confidential Information and any other material posted to any forum, newsgroup, chat, instant messaging session, text message, Internet page or other Internet communication by any Employee in the course of his or her Company duties.
20. Employees should immediately report any suspected violations of this Policy to their immediate supervisor, the next level of management, or the appropriate Access Manager, or other appropriate personnel, such as the Director, in accordance with the Code, the applicable Employee handbook, and this Policy, or otherwise to the Company via the Sims Metal Management Ethics & Compliance Hotline (as outlined in the Code).
21. Employees who fail to comply with this Policy may be subject to disciplinary action by the Company and other consequences, as set out at the start of this Policy. Employees releasing protected Confidential Information via an Internet newsgroup, chat session, instant messaging session, text message or other Internet communication – whether or not the release is inadvertent – may be subject to Company disciplinary action in accordance with applicable Company policy.
22. The Company reserves the right to amend this Internet Usage Policy at any time and will issue or make available revised versions to relevant Employees.

**SIMS METAL MANAGEMENT INFORMATION SECURITY POLICY
EMPLOYEE ACKNOWLEDGMENT FORM**

I have received a copy Sims Metal Management's Information Security Policy (Policy). I agree to read it in full and to ask my immediate supervisor or the Group Director of Information Technology, or his/her delegate in my region, if I have any questions about this Policy. I acknowledge my understanding of this Policy and agree to comply with it in all respects.

Date

Employee Signature

Business Unit Location

Employee Name (please print or type)

FILE SIGNED ACKNOWLEDGMENT FORM IN PERSONNEL FILE