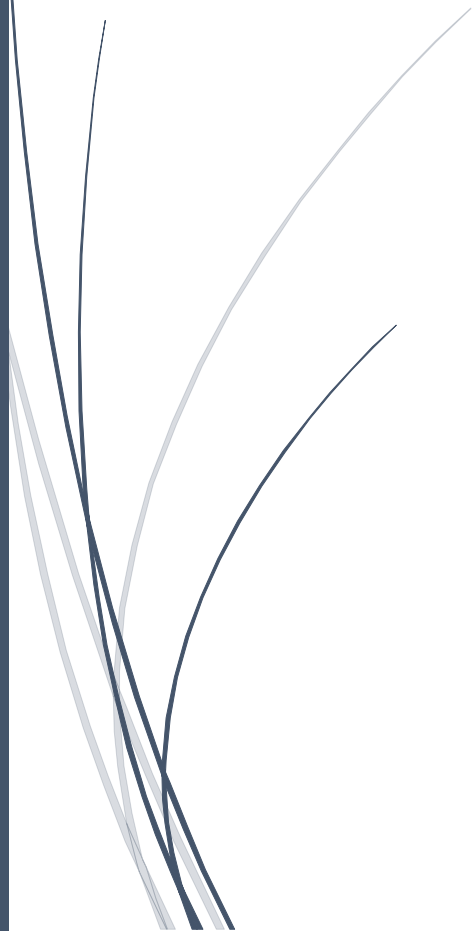
09 September 2015

StrathTech Privledged Access Agreement



Adam McGhie
STRATHTECH SYSTEMS ADMIN

Contents

INTRODUCTION

Privileged access enables an individual to take actions which may affect computing systems, network communication, or the accounts, files, data, or processes of other users. Privileged access is typically granted to system administrators, network administrators, members performing computing account administration, or other such employees whose job duties require special privileges over a computing system or network.

Individuals with privileged access must respect the rights of the system users, respect the integrity of the systems and related physical resources, and comply with any relevant laws or regulations. Individuals also have an obligation to keep themselves informed regarding any procedures, business practices, and operational guidelines pertaining to the activities of their local department.

In particular, the principles of academic freedom, freedom of speech, and privacy of information hold important implications for computer system administration at StrathTech. Individuals with privileged access must comply with applicable policies, laws, regulations, precedents, and procedures, while pursuing appropriate actions required to provide high-quality, timely, reliable, computing services. For example, individuals must comply with provisions of the University of Strathclyde Legal Framework for ICT (LFICT) mandating the least perusal of contents and the least action necessary to resolve a situation.

GENERAL PROVISIONS

1. Privileged access is granted only to authorized individuals. Privileged access shall be granted to individuals only after they have read and signed this Agreement.
2. Privileged access may be used only to perform assigned job duties.
3. If methods other than using privileged access will accomplish an action, those other methods must be used unless the burden of time or other resources required clearly justifies using privileged access.
4. Privileged access may be used to perform standard system-related duties only on machines and networks whose responsibility is part of assigned job duties. Examples include:
    a. installing system software;
    b. relocating individuals' files from critically overloaded locations;
    c. performing repairs required to return a system to normal function, such as fixing files or file processes, or killing runaway processes;
5. running security checking programs;
6. Monitoring the system to ensure reliability and security.
7. Privileged access may be used to grant, change, or deny resources, access, or privilege to another individual only for authorized account management activities or under exceptional

circumstances. Such actions must follow any existing organizational guidelines and procedures. Examples include:

8. disabling an account apparently responsible for serious misuse such as: attempting to compromise root (UNIX) or the administrator account (Windows), using a host to send harassing or threatening email, using software to mount attacks on other hosts, or engaging in activities designed to disrupt the functioning of the host itself;
9. disconnecting a host or subnet from the network when a security compromise is suspected;
10. Accessing files for law enforcement authorities with a valid subpoena.

In the absence of compelling circumstances, the investigation of information in, or suspension of, an account suspected to be compromised should be delayed until normal business hours to allow appropriate authorization and/or notification activities.

In all cases, access to other individuals' electronic information shall be limited to the least perusal of contents and the least action necessary to resolve a situation.

Individuals with privileged access shall take necessary precautions to protect the confidentiality of information encountered in the performance of their duties.

If, during the performance of their duties, individuals with privileged access inadvertently see information indicating serious misuse, they are advised to consult with the Elected Systems Admin or the President. If the situation is an emergency, intervening action may be appropriate.

The LFICT governs all activities using StrathTech electronic communication resources. LFICT provisions must be followed when electronic communication records are involved in any situation.

AUTHORIZATION

Under most circumstances, the consent of the holder of an electronic communications record (see LFICT) must be obtained before accessing their files or interfering with their processes. If consent cannot be obtained, then LFICT conditions for "Access Without Consent" must be met.

NOTIFICATION

In either case, the member or other authority shall, at the earliest opportunity consistent with law and University policy, attempt to notify the affected individual(s) of the action(s) taken and the reasons for those action(s).

RECOURSE

If conflicts or disputes arise regarding activities related to this Agreement, individuals may pursue their rights to resolve the situation through existing procedures. Such procedures would include informal supervisory or departmental conflict resolution procedures, relevant provisions of employment policies or contracts, student or faculty conduct procedures, or other such documents which pertain to the particular individual's affiliation with the University.

AGREEMENT

I have read this Privileged Access Agreement, the University of Strathclyde Legal Framework for ICT.

I agree to comply with the provisions of this Privileged Access Agreement, the University of Strathclyde Legal Framework for ICT, and any relevant University of Strathclyde Computer Use Policies.

Signature _____

Print Name _____

Date _____

Systems or Resources Approved for Privileged Access:

_____

_____

_____

_____

Authorizing Signature _____

Print Name _____

Date _____