Information Security Policy
British Educational Research Association

Company Limited by Guarantee

Company Number 08284220, Registered Charity Number 1150237

Updated November 2020

BERA Information Security Policy

Purpose

1. This policy exists to support BERA in its management of information risk, providing strategic guidance, advice, and support. Regardless of the form it takes, or means by which it is shared or stored, information should always be protected appropriately.

2. Information security is characterized here as being concerned with guaranteeing availability (ensuring that authorized users always have access to information when they need it), integrity (safeguarding its accuracy and completeness), confidentiality (ensuring that sensitive information is accessible only to those authorized to use it), and authenticity.

3. This policy applies to all staff (temporary or permanent), members and volunteers of BERA who are granted access to information systems. BERA staff also employed by University College London (UCL) must also adhere to their Information Security Policy and make themselves aware of this.

4. Should any further information be required, or to discuss this policy, please contact Nick Johnson, Chief Executive.

Responsibilities for Information Security

5. All those who make use of BERA's systems and information, electronic or otherwise, have a responsibility for protection of these assets. Individuals must, at all times, act in a responsible and professional manner and refrain from any activity that may jeopardise security.

6. It is the responsibility of each individual to ensure his/her understanding of and compliance with this policy and any associated procedures or codes of practice.

7. The User will not share usernames and passwords, unless necessary, with other individuals for any IT system, including the BERA website, other website logins and the Customer Relationship Manager (CRM). The User will undertake reasonable means to ensure the safety of passwords. Prior to any necessary sharing of details, both users must be aware of what is expected of them with regards to the Security Policy.

8. Any facility (including software) provided is used entirely at the risk of the User. BERA is not liable for any loss, damage or inconvenience arising directly or indirectly from the use of computer facilities.

Compliance with legislation

9. BERA staff, members and authorised third parties, have an obligation to abide by all UK legislation and the relevant legislation of the European Union. Of particular importance in this respect are the Computer Misuse Act 1990, the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000, the Terrorism Act 2006 and the Counter Terrorism and Security Act 2015.

10. This policy satisfies the Data Protection Act's requirement for a formal statement of BERA's security arrangements for personal data. The requirement for compliance devolves to all users defined in this policy, who may be held personally responsible for any breach of the legislation.

Breaches of security

11. Any individual suspecting the security of the computer system has been breached must contact BERA's IT provider, BERA's data protection officer (BERA Membership and Engagement Manager) and BERA's Chief Executive.

12. BERA's IT provider may then require unsafe systems are removed or made inaccessible. Applications may be recovered from a pre-incident backup to ensure a clean system going forward.

13. Physical security breaches must be reported to UCL Estates security team and BERA's Chief Executive.

14. BERA's Chief Executive has the authority to take necessary action to protect BERA from breaches of security.

15. BERA undertakes appropriate security measures against unauthorised access to, or alteration, disclosure or destruction, or accidental loss of personal or other data it does not operate a high security system and cannot and does not give any warranties about security or confidentiality of data, personal or other.

Policy awareness

16. Existing and new staff, authorised third parties and contractors given access to the BERA network and data will be advised of the existence of this policy statement and the availability of the associated procedures, codes of practice and associated policies. Failure of an individual to comply with this policy may lead to the instigation of disciplinary procedures and, in certain circumstances, legal action may be taken. Failure of a contractor to comply could lead to the cancellation of a contract.

17. BERA reserve the right to withdraw permission to use the facilities provided and take any other relevant action in the event of any abuse of the facilities by the User.

18. BERA is the owner of all email addresses used by the company and reserve the right to access or reclaim any emails or files upon termination of your employment or notice of resignation with BERA.

19. In the event of a medium to long-term absence, BERA will endeavour to seek the permission of the User before accessing any emails or files needed, however BERA may use their discretion at any point to access any information required.

Associated policies

- BERA Data Protection Policy
- BERA Ransomware Guidance – Internal Policy
- BERA Email retention Policy – Internal Policy
- Other policies as appropriate

This policy is not exhaustive and can be updated at any time.