# BASDA Software Security – Code of Practice Guide (v1.0)

## Introduction

As BASDA members, we recognise the fundamental importance of secure use of software. Such secure use can be facilitated by the software design but is also critically dependent on the way the software is implemented and used (which is the responsibility of the user rather than the software vendor). We will strive to apply the following software design principles and to inform our users of the following recommended software usage principles.

| Software Design Principles | Recommended Software Usage Principles |
|---|---|
| **1 Data Protection Legislation Compliance** | |
| Software should be designed to enable and facilitate compliance with the Data Protection Act 1998 (together with any other relevant legislation) as it applies to the processes and data which the software is designed to handle. | Users of software should be aware of their responsibility to comply with the Data Protection Act 1998 (together with any other relevant legislation) as it applies to the processes and data which they handle. |
| **2 Software Function and Data Access Controls** | |
| Software should be designed to allow suitable control over access to the application as a whole and, where appropriate, to specific application functions and stored data taking into account the purpose, usage and sensitivity of the data and processes involved together with the scale and complexity of the software application. This may be provided by passwords, user profiles, group profiles, and/or other suitable means. | Users of software should apply suitable control over access to the application as a whole and, where appropriate, to specific application functions and stored data, taking into account the purpose, usage and sensitivity of the data and processes required for each user's role together with the scale and complexity of the software application. This may be applied by passwords, user profiles, group profiles, and/or other suitable means. Users should ensure that all passwords are appropriately complex, kept secret and changed frequently. |
| **3 Authorisation of Data Submitted to Banks and Statutory Authorities** | |
| Where software is designed to submit data to banks and/or statutory authorities (including electronic payment instructions, tax returns, statutory forms, etc.) it should be designed to ensure that appropriate controls are available for the authorisation and secure handling of such submissions. | Where software is used to submit data to banks and/or statutory authorities (including electronic payment instructions, tax returns, statutory forms, etc) they should ensure that appropriate controls are applied for the authorisation and secure handling of such submissions. |
| **4 Data Storage and Audit Trails** | |
| Software should be designed to ensure that data is stored in a form which is appropriate with regard to the nature of the information held and the security considerations relating to it. Suitable audit trail facilities should be provided to track changes to important data where required by the scale and nature of the intended use of the software. | Users of software should ensure that data is stored in a form which is appropriate with regard to the nature of the information held and the security considerations relating to it. Appropriate use should be made of any audit trail facilities to track changes to important data, particularly where there are significant numbers of users of the software. |
| **5 Data Backup and Recovery** | |
| Software should be designed with due regard to the importance of data backup and recovery. These facilities may be provided either within the software itself or externally in the operating system or other third-party application. | Users of software should take responsibility for ensuring that all business data are backed up securely and at an appropriate frequency. Data recovery should be tested periodically. |

***I certify that our solutions meet this Code of Practice***

| | | | |
|---|---|---|---|
| **Name** | | **Title** | |
| **Member** | | **Date** | |

Published by: BASDA 92 High Street Great Missenden Buckinghamshire HP16 0AN

Tel: +44 (0) 1494 868030 Fax +44 (0) 1494 868031 Email: info@basda.org Web: www.basda.org

# BASDA Software Security – Code of Practice Guide (v1.0)

## Member entitlements of signing-up to this code of practice

Promotion on the members' web site of BASDA issued logo, which routes any click direct to the BASDA primary site and the code of practice, as per page 1 of this document. Members may also publish this on relevant marketing collateral – digital and physical.

The above entitlement exists while:

- Membership is retained, via timely annual renewal of BASDA membership
- Members have self-certified their conformance with this CoP, and renewed this every two years
- No significant ongoing security issues exist that fundamentally breach this CoP, as brought to BASDA's attention

## FAQs

**Q**. How often will this CoP be updated?

***A***. *The CoP will be reviewed annually and modified, if appropriate. Should exceptional circumstances arise then that may also trigger an ad hoc change.*

**Q**. How will members know if it has changed?

***A***. *BASDA will notify members, with as much advance notice as is possible so as to ensure ongoing compliance.*

**Q**. What will members need to do in regard to their web site?

***A***. *No action will be required; the automatic link built into the logo routes through to the BASDA site, which will be automatically updated following advance notification to members.*

**Q**. What happens if a breach of the CoP is reported to BASDA?

***A***. *BASDA will advise the member and expects the issues to be resolved in a very timely issue and should this not be satisfactorily resolved then BASDA retains the right to remove the member's entitlements under this CoP. BASDA will then check that the logo and accompanying references are removed from the members' web site and all other collateral.*

**Q**. How do members apply?

***A***. *Members should review their solutions' security against the CoP and on the basis that the member is fully confident that it meets the CoP then a senior, named manager (e.g. Head of R&D) –with the delegated authority of that Member – needs to complete the certification box (p1) and e-mail this document to: admin@basda.org.uk*

**Q**. What confirmation do I receive and when can we publish the logo?

***A***. *Upon receipt of completed forms, BASDA will confirm the member's entitlement, duration (i.e. self-certification renewal date) and issue the logo and accompanying details to the certifying member contact.*

**Q**. What if the certifying individual is no longer with the member at time of required renewal?

***A***. *BASDA will also contact its primary contact point alongside the nominated member contact to best help the member take advantage of the renewal opportunity.*

**Q**. What are the application limitations of CoP?

***A***. *This CoP is primarily focused upon business applications and those that interact with regulatory bodies, such as government and banks however, the principles apply to many other applications, inc. consumer based ones. The term software is a generic one and does not limit the application as to how it is deployed.*



Tel: +44 (0) 1494 868030 Fax +44 (0) 1494 868031 Email: info@basda.org Web: www.basda.org