Access Control Policy

1.0 Overview

- This Access Control policy defines the rules, rights and restrictions applied to users for both logical and physical access to the organisation's assets.

1.1 Principles

- **Need-to-know:** you are only granted access to the information you need to perform your tasks(different tasks/roles mean different need-to-know and hence different access profile).
- **Need-to-use:** you are only granted access to the information processing facilities (IT equipment, applications, procedures, rooms) you need to perform your task/job/role.

2.0 Policy

2.1 Security of Systems

- The organization uses several systems to operate effectively, and it's important tomaintain the confidentiality, integrity and availability of these information assets through this access control policy.
- Threats associated with the information assets have been considered and addressed as far as possible through the risk management process.

2.2 Security of Networks and Services

- Access to the organisations networks shall be limited to prevent unauthorized and unintended consequences.
- Devices will not be connected to the network without authorization from the **IT Support Company**.
- The WIFI connection details will not be shared without the authorization of the **IT Support Company.**
- Guests, visitors and third parties will use ONLY the **visitor WIFI network** madeavailable.

2.3 Physical Security

- The physical security of the organisation's assets, including buildings and offices, should be considered at all times.
- Please ensure the main door is closed and secure, do not leave it ajar. All visitors and third parties must report to reception and sign in.

- Challenge any strangers on-site who do not appear to be accompanied.

2.4 Access Requests

- Access requests, including new user accounts, should be submitted to the **IT Support Company** by email.

- The job functions as described by the department manager should be reviewed to ensure that the requested access is relevant and acceptable. In the case of IT systems including Active Directory, a profile including privileges may be copied from a colleague with the same job functions.

2.5 Access Authorisation

- The managing director has overall governance of access control within the company and May, for legitimate business reasons, grant or revoke access at their discretion.

- Department managers are responsible for determining the access levels required by their staff and should, where possible, maintain security groups.

2.6 Access Administration

- When an access request has been approved by the Gatekeeper, a record of that decision will be maintained to allow an audit trail.

- The gatekeeper will provide access to the user and inform them via an appropriate method, so as to keep any username separate from a password.

- Where systems allow, a temporary password will be used and the user will be required to change their password at first log-in.

2.7 Access Review

- The access to systems will be reviewed on a regular basis to ensure that users are still authorized to access each system and that the privilege level assigned to that user is still acceptable.

- Gatekeepers will be responsible for reviewing their own systems and may need to refer to department managers for confirmation of user requirements.

2.8 Access Removal

- In cases of disciplinary or where an employee is within their probation period, access should be removed immediately.

- Where a notice period has been agreed, or the user is changing job function within the company, access should be removed when it has been confirmed by their line manager.

2.9 Privileged Access

- All privileged access should be reviewed against the job function before the details or assets (including access cards/fobs) are issued to the user.
- The use of privileged accounts will be limited and uniquely identifiable username will be used to enable all activity under an account to the traced back to a single individual.

2.10 Logging & Monitoring

- User activity is logged and may be monitored for the purposes of error detection and security.

3. System Gatekeepers

- The organisation uses several systems to store data, and these are administered by different peoplein the organisation. The table below shows the gatekeepers of those systems, who you should go tofor any of the above issues.

System	Gatekeeper	Review Frequency
Active Directory	MD / IT Support	Annual
Mail Server	MD / IT Support	Annual
Sage Line 50	MD / Accounts	Annual
Iris Payroll	MD / Accounts	Annual
Intruder Alarm	MD	Annual
Website (Front)	MD / Web Dev	Annual
Website (DB)	MD / Web Dev	Annual
WIFI	MD / IT Support	Annual

Enhancements for Access Control Policy:

1. Incorporating **least privilege** and **separation of duties** concepts.
2. Enforcing **password complexity** and **multi-factor authentication (MFA)**.
3. Conducting **regular network monitoring** and **vulnerability assessments**.
4. Implementing **role-based access control (RBAC)** for consistency.

Data Protection and Data Security Policy

Statement and purpose of policy

A. Bandweaver Technology Limited (the **Employer**) is committed to ensuring that all personal data handled by us will be processed according to legally compliant standards of data protection and data security.

B. We confirm for the purposes of the data protection laws, that the Employer is a data controller of the personal data in connection with your employment. This means that we determine the purposes for which, and the manner in which, your personal data is processed.

C. The purpose of this policy is to help us achieve our data protection and data security aims by:

1. notifying our staff of the types of personal information that we may hold about them, our customers, suppliers and other third parties and what we do with that information;
2. setting out the rules on data protection and the legal conditions that must be satisfied when we collect, receive, handle, process, transfer and store personal data and ensuring staff understand our rules and the legal standards; and
3. clarifying the responsibilities and duties of staff in respect of data protection and data security.

D. This is a statement of policy only and does not form part of your contract of employment. We may amend this policy at any time, in our absolute discretion.

E. E. For the purposes of this policy:

1. **Criminal records data** means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.
2. **Data protection laws** means all applicable laws relating to the processing of Personal Data, including, for the period during which it is in force, the General Data Protection Regulation (Regulation (EU) 2016/679).
3. **Data subject** means the individual to whom the personal data relates.
4. **Personal data** means any information that relates to an individual who can be identified from that information.
5. **Processing** means any use that is made of data, including collecting, storing, amending, disclosing, or destroying it.
6. **Special categories of personal data** means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

Data protection principles

1. Staff whose work involves using personal data relating to Staff or others must comply with this policy and with the following data protection principles which require that personal information is:
   a. **processed lawfully, fairly and in a transparent manner.** We must always have a lawful basis to process personal data, as set out in the data protection laws. Personal data may be processed as necessary to perform a contract with the data subject, to comply with a legal obligation which the data controller is the subject of, or for the legitimate interest of the data controller or the party to whom the data is disclosed. The data subject must be told who controls the information (us), the purpose(s) for which we are processing the information and to whom it may be disclosed.
   b. **collected only for specified, explicit and legitimate purposes.** Personal data must not be collected for one purpose and then used for another. If we want to change the way we use personal data, we must first tell the data subject.
   c. **processed only where it is adequate, relevant and limited to what is necessary for the purposes of processing.** We will only collect personal data to the extent required for the specific purpose notified to the data subject.
   d. **accurate and the Employer takes all reasonable steps to ensure that information that is inaccurate is rectified or deleted without delay.** Checks to personal data will be made when collected and regular checks must be made afterwards. We will make reasonable efforts to rectify or erase inaccurate information.
   e. **kept only for the period necessary for processing.** Information will not be kept longer than it is needed and we will take all reasonable steps to delete information when we no longer need it. For guidance on how long particular information should be kept, contact the To be confirmed, or request a copy of our Data retention policy.
   f. **secure, and appropriate measures are adopted by the Employer to ensure as such.**

Who is responsible for data protection and data security?

2. Maintaining appropriate standards of data protection and data security is a collective task shared between us and you. This policy and the rules contained in it apply to all staff of the Employer, irrespective of seniority, tenure and working hours, including all employees, directors and officers, consultants and contractors, casual or agency staff, trainees, homeworkers and fixed-term staff and any volunteers (**Staff**).

3. Questions about this policy, or requests for further information, should be directed to the To be confirmed.

4. All Staff have personal responsibility to ensure compliance with this policy, to handle all personal data consistently with the principles set out here and to ensure that measures are taken to protect the data security. Managers have special responsibility for leading by example and monitoring and enforcing compliance. The To be confirmed must be notified if this policy has not been followed, or if it is suspected this policy has not been followed, as soon as reasonably practicable.

5. Any breach of this policy will be taken seriously and may result in disciplinary action up to and including dismissal. Significant or deliberate breaches, such as accessing Staff or customer personal data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

What personal data and activities are covered by this policy?

6. This policy covers personal data:
   a. which relates to a natural living individual who can be identified either from that information in isolation or by reading it together with other information we possess;
   b. is stored electronically or on paper in a filing system;
   c. in the form of statements of opinion as well as facts;
   d. which relates to Staff (present, past or future) or to any other individual whose personal data we handle or control;
   e. which we obtain, is provided to us, which we hold or store, organise, disclose or transfer, amend, retrieve, use, handle, process, transport or destroy.
7. This personal data is subject to the legal safeguards set out in the data protection laws.

What personal data do we process about Staff?

8. We collect personal data about you which:
   a. you provide or we gather before or during your employment or engagement with us;
   b. is provided by third parties, such as references or information from suppliers or another party that we do business with; or
   c. is in the public domain.
9. The types of personal data that we may collect, store and use about you include records relating to you:
   a. home address, contact details and contact details for your next of kin;
   b. recruitment (including your application form or curriculum vitae, references received and details of your qualifications);
   c. pay records, national insurance number and details of taxes and any employment benefits such as pension and health insurance (including details of any claims made);
   d. telephone, email, internet, fax or instant messenger use;
   e. performance and any disciplinary matters, grievances, complaints or concerns in which you are

involved.

f. We may also hold passport copies, and visa scans, copy of driving license or other identity document.

Sensitive personal data

10. We may from time to time need to process sensitive personal information (sometimes referred to as 'special categories of personal data').
11. We will only process sensitive personal information if:
    a. we have a lawful basis for doing so, eg it is necessary for the performance of the employment contract; and
    b. one of the following special conditions for processing personal information applies:
        i. the data subject has given explicit consent.
        ii. the processing is necessary for the purposes of exercising the employment law rights or obligations of the Company or the data subject.
        iii. the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent.
        iv. processing relates to personal data which are manifestly made public by the data subject.
        v. the processing is necessary for the establishment, exercise, or defence or legal claims; or vi. the processing is necessary for reasons of substantial public interest.
12. Before processing any sensitive personal information, Staff must notify a company director or authorized HR representative of the proposed processing, in order for this person to assess whether the processing complies with the criteria noted above.
13. Sensitive personal information will not be processed until the assessment above has taken place and the individual has been properly informed of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.
14. Our privacy notice sets out the type of sensitive personal information that we process, what it is used for and the lawful basis for the processing.

Criminal records information

15. Criminal records information will be processed as part of the employment recruitment process and ongoing due diligence either due to company policy or requests from 3rd parties (e.g. customers, banks…).

How we use your personal data

16. We will tell you the reasons for processing your personal data, how we use such information and the legal basis for processing in our privacy notice. We will not process Staff personal information for any other reason.
17. In general we will use information to carry out our business, to administer your employment or engagement and to deal with any problems or concerns you may have, including, but not limited to:
    a. **Staff Address Lists:** to compile and circulate lists of home address and contact details, to contact you outside working hours.
    b. **Sickness records:** to maintain a record of your sickness absence and copies of any doctor's notes or other documents supplied to us in connection with your health, to inform your colleagues and others that you are absent through sickness, as reasonably necessary to manage your absence, to deal with

unacceptably high or suspicious sickness absence, to inform reviewers for appraisal purposes of your sickness absence level, to publish internally aggregated, anonymous details of sickness absence levels.

c. **Monitoring IT systems:** to monitor your use of e-mails, internet, telephone and fax, computer or other communications or IT resources.

d. **Disciplinary, grievance or legal matters:** in connection with any disciplinary, grievance, legal, regulatory or compliance matters or proceedings that may involve you.

e. **Performance Reviews:** to carry out performance reviews.

f. **Business Operations:** Applications for visas, letter of invitations etc. for business travel (Passport). Applications for permits etc. for access to customer sites (Identity documents).

g. Submission of employee CVs to customers during bids for winning business. (CV)

Accuracy and relevance

18. We will:

a. ensure that any personal data processed is up to date, accurate, adequate, relevant and not excessive, given the purpose for which it was collected.

b. not process personal data obtained for one purpose for any other purpose, unless you agree to this or reasonably expect this.

19. If you consider that any information held about you is inaccurate or out of date, then you should tell your line manager. If they agree that the information is inaccurate or out of date, then they will correct it promptly. If they do not agree with the correction, then they will note your comments.

Storage and retention

20. Personal data (and sensitive personal information) will be kept securely in accordance with our Information Security Policy.

21. The periods for which we hold personal data are contained in our privacy notices.

Data security

22. We will use appropriate technical and organisational measures to keep personal data secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

23. Maintaining data security means making sure that:

a. only people who are authorised to use the information can access it;

b. where possible, personal data is pseudonymised or encrypted;

c. information is accurate and suitable for the purpose for which it is processed; and

d. authorised persons can access information if they need it for authorised purposes.

24. By law, we must use procedures and technology to secure personal information throughout the period that we hold or control it, from obtaining to destroying the information.

25. Personal information must not be transferred to any person to process (eg while performing services for us on or our behalf), unless that person has either agreed to comply with our data security procedures or we are satisfied that other adequate measures exist.

26. Security procedures include:

a. Any desk or cupboard containing confidential information must be kept locked.

b. Computers should be locked with a strong password that is changed regularly or shut down when they are left unattended and discretion should be used when viewing personal information on a monitor to ensure that it is not visible to others.

c. Data stored on CDs or memory sticks must be encrypted or password protected and locked away securely when they are not being used.

d. The Director or IT Manager must approve of any cloud used to store data.

e. Data should never be saved directly to mobile devices such as laptops, tablets or smartphones.

f. All servers containing sensitive personal data must be approved and protected by security software.

g. Servers containing personal data must be kept in a secure location, away from general office space.

h. Data should be regularly backed up in line with the Employer's back-up procedure.

27. Telephone Precautions. Particular care must be taken by Staff who deal with telephone enquiries to avoid inappropriate disclosures. In particular:

a. the identity of any telephone caller must be verified before any personal information is disclosed;

b. if the caller's identity cannot be verified satisfactorily then they should be asked to put their query in writing;

c. do not allow callers to bully you into disclosing information. In case of any problems or uncertainty, contact your line manager.

28. Methods of disposal. Copies of personal information, whether on paper or on any physical storage device, must be physically destroyed when they are no longer needed. Paper documents should be shredded and CDs or memory sticks or similar must be rendered permanently unreadable.

29. Additional measures to ensure data security include Use of Virtual Private Networks . See communications and use of equipment policy

Data impact assessments

30. Some of the processing that the Employer carries out may result in risks to privacy.

31. Where processing would result in a high risk to Staff rights and freedoms, the Employer will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

Data breaches

32. If we discover that there has been a breach of Staff personal data that poses a risk to the rights and freedoms of individuals, we will report it to the Information Commissioner within 72 hours of discovery.

33. We will record all data breaches regardless of their effect in accordance with our Breach response policy.

34. If the breach is likely to result in a high risk to your rights and freedoms, we will tell affected individuals that there has been a breach and provide them with more information about its likely consequences and the mitigation measures it has taken.

Individual responsibilities

35. Staff are responsible for helping the Employer keep their personal data up to date.

36. Staff should let the Employer know if personal data provided to the Employer changes, eg if you move house or change your bank details.

37. You may have access to the personal data of other Staff members and of our customers in the course of your employment. Where this is the case, the Employer relies on Staff members to help meet its data protection obligations to Staff and to customers.

38. Individuals who have access to personal data are required:

a. to access only personal data that they have authority to access and only for authorised purposes;

b. not to disclose personal data except to individuals (whether inside or outside of the Employer) who have appropriate authorisation;

c. to keep personal data secure (eg by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);

d. not to remove personal data, or devices containing or that can be used to access personal data, from the Employer's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and

e. not to store personal data on local drives or on personal devices that are used for work purposes.

Training

39. We will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.

40. Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy will receive additional training to help them understand their duties and how to comply with them.

Enhancements for Data Protection and Security Policy:

1. Data Retention period is not clearly stated in this document. Incorporating this information or providing direct access to the retention policy would strengthen transparency.

2. More attention could be placed on practical awareness and phishing prevention. Consider periodic real-world simulations to keep staff prepared for social engineering attacks.

3. Expanding on when and how anonymization and pseudonymization are applied could provide clarity on safeguarding personally identifiable information (PII) at different stages of processing.

4. It could benefit from more specific rules about the types of cloud platforms allowed (e.g., ensuring they comply with ISO 27001 or equivalent standards), along with clear guidance for remote workers or employees using their own devices.

5. Integrating more focus on "Privacy by Design" principles, ensuring that data protection is considered from the start of any new project or system implementation. Including these considerations in the policy encourages the proactive protection of privacy.