Third-Party Administrator Access

Policy & Customer Liability Acknowledgement

A Message From Our Team

Thank you for choosing SMB Solutions Cloud Services to host your SAP Business One environment. We genuinely care about keeping your business running smoothly, and that means being open and honest with you when it comes to decisions that could affect the security, stability, and compliance of your hosted system.

One of those topics is granting administrative-level access to your hosted environment to third parties — such as external SAP consultants, implementation partners, or software vendors.

This document explains our position on third-party admin access in plain language, offers our recommended approach, and — if you choose to proceed — provides a formal acknowledgement for you to sign.

Why We Don't Recommend Unsupervised Third-Party Admin Access

We understand the convenience of allowing a consultant or software vendor to "just log in and sort it out." But from our experience managing cloud-hosted SAP environments, unsupervised admin access by third parties introduces risks that are worth understanding before you decide.

Security & Compliance

- Your environment is hosted within Equinix-grade infrastructure and operates under SMB Solutions' ISO/IEC 27001:2022 certification and SOC 2 Type II attestation. Granting external admin credentials — particularly without audit oversight — can conflict with the principles of both frameworks and your own obligations as a data controller.
- We have no visibility into the security practices of third-party organisations. Compromised credentials on their side can become a direct threat to your data.
- Admin-level access allows a third party to view, export, or modify any data in your system — including sensitive financial, customer, and employee records.

SOC 2 Certification — What This Means for You

SMB Solutions Cloud Services holds SOC 2 Type II attestation, which means our security controls, availability, confidentiality, and operational practices are independently audited on an ongoing basis. This is one of the most rigorous cloud security standards available and it is a key reason our customers trust us with their business-critical SAP environments.

Granting unsupervised admin access to a third party has direct implications for this certification and for the protections it provides you:

- SOC 2 requires that access to systems containing sensitive data is strictly controlled, monitored, and limited to authorised personnel. Introducing an unvetted third party with admin rights creates access control gaps that fall outside the scope of our audited environment.
- Our SOC 2 audit trail covers activity by SMB Solutions personnel and systems. Actions taken by a third party using separately provisioned credentials will appear in logs but are outside our control boundary — meaning we cannot attest to or be accountable for their actions.
- If a security incident occurs that is traceable to third-party admin activity, it may jeopardise SMB Solutions' ability to provide a clean SOC 2 attestation report — which in turn could affect the assurances we are able to provide to all of our customers, including you.
- Your own organisation may have compliance obligations — such as under the Australian Privacy Act, industry regulations, or contractual requirements with your customers — that require you to ensure that any parties with access to your data operate under equivalent security standards. A third party without comparable certifications may not meet that bar.

Our Certifications at a Glance

ISO/IEC 27001:2022 — International standard for information security management systems (ISMS).

SOC 2 Type II — Independent attestation that our security, availability, and confidentiality controls operate effectively over time.

Both certifications are maintained through continuous auditing and apply to the infrastructure and processes that protect your hosted environment.

Introducing unvetted third-party access places activity outside the boundaries of these certified controls.

System Stability

- Unauthorised or poorly tested configuration changes made by third parties at the admin level are one of the most common causes of system instability in hosted SAP environments.
- Changes to system settings, integrations, user permissions, or add-ons can have unintended downstream consequences that are costly and time-consuming to diagnose and reverse.
- SMB Solutions cannot be held responsible for issues arising from changes made by parties outside our control.

Licensing & Cost Implications

- Creating additional user accounts to accommodate third-party access may trigger additional SAP Business One licence requirements, which incur real costs.
- Hosting resource usage, bandwidth, and support time associated with third-party activity will be attributed to your account and may affect your hosting fees.
- Any remediation work required as a result of third-party changes will be billable at standard rates.

Our Recommendation: Supervised Access

We **strongly encourage** you to supervise all third-party activity within your hosted environment. Here's what that looks like in practice:

✔ Recommended Approach for Third-Party Access

1. Have a member of your team present (in person or via screen share) while the third party works in your system.
2. Use a dedicated, temporary user account for the third party rather than sharing existing admin credentials.
3. Set a defined scope and timeframe for the access — and remove or disable the account when the work is done.
4. Request a summary of all changes made from the third party upon completion of their work.
5. Contact our support team before granting access so we can advise on the safest approach for your specific environment.

This approach gives you the access you need while maintaining control, accountability, and a clear audit trail. Our team is always happy to assist with setting up temporary accounts or advising on best-practice access configurations.

⚠ Before You Proceed

If you choose to grant unsupervised admin access to a third party, please read and sign the Liability Acknowledgement below.

By signing, you confirm that you understand and accept responsibility for any issues, costs, and consequences that arise from this decision.

SMB Solutions **strongly advises** against unsupervised third-party admin access and accepts no liability for any resulting issues.

Customer Liability Acknowledgement

Third-Party Admin Access to Hosted SAP Business One Environment

Customer Name	
Company Name	
Third-Party Name / Org	
Purpose of Access	
Date	

Acknowledgement of Risk & Acceptance of Liability

I, the undersigned, as an authorised representative of the Customer named above, hereby acknowledge and confirm the following:

1. I have been informed of SMB Solutions Cloud Services' recommendation against granting unsupervised administrative access to hosted SAP Business One environments to third-party individuals or organisations.
2. I understand that granting third-party admin access introduces risks including, but not limited to data security exposure, system instability, unauthorised configuration changes, compliance risks, unplanned costs, and potential impacts on SMB Solutions' ISO/IEC 27001:2022 and SOC 2 Type II certification boundaries.
3. I understand that SMB Solutions' SOC 2 Type II attestation covers controls operated by SMB Solutions personnel and systems. Actions taken by a third party with admin access operate outside the certified control boundary, and SMB Solutions cannot be held accountable for such actions or their impact on compliance obligations — mine or those of SMB Solutions.
4. I accept responsibility for ensuring that any third party granted access to my hosted environment meets security and compliance standards appropriate for handling the data contained within that environment, and I acknowledge that SMB Solutions makes no representation regarding the security practices of any such third party.
5. I accept full responsibility for any and all issues arising directly or indirectly from the granting of third-party admin access to my hosted SAP Business One environment, including but not limited to: data loss, data corruption, system outages, security breaches, and non-compliance with applicable laws or regulations.
6. I accept full financial responsibility for any costs incurred as a result of third-party activity in my hosted environment, including additional SAP Business One licence fees, additional hosting fees, support and remediation labour charges billed at SMB Solutions' standard rates, and any third-party costs incurred during recovery or remediation.
7. I agree to indemnify and hold SMB Solutions Cloud Services, its directors, employees, and subcontractors harmless from any claim, loss, liability, cost, or expense arising from the granting of this third-party access.
8. I understand that SMB Solutions Cloud Services will provide reasonable assistance to resolve issues caused by third-party access, and that all such assistance will be

billable at standard support rates unless otherwise covered by an existing managed services agreement.

9. I confirm I am authorised to sign this acknowledgement on behalf of the Customer and to bind the Customer to its terms.

Customer Signature

Authorised Signatory (Full Name)	*Title / Position*
Signature	*Date*

SMB Solutions Acknowledgement (Internal Use)

SMB Solutions Representative (Full Name)	*Title / Position*
Signature	*Date*

